NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

RISK QUANTIFICATION OF SYSTEMS ENGINEERING DOCUMENTS IMPROVES PROBABILITY OF DOD PROJECT SUCCESS

by

Thomas C. Irwin

September 2009

Thesis Advisor:	Walter Owen
Second Reader:	John Gay

Approved for public release; distribution is unlimited

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** September 2009	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Risk Quantification of Systems Engineering Documents Improves Probability of DoD Project Success		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Thomas C. Irwin			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE**	

13. ABSTRACT (maximum 200 words)

A frame transition problem exists between project Systems Engineers (SE) and Department of Defense (DoD) Program Managers (PM). Systems engineering organizations, operating in a rational frame, must produce technical documents required for the PM operating in a political frame of constrained resources. These artifacts, required for milestone reviews, are the results of extensive technical effort that must be accounted for and adequately resourced during project planning by the PM. Programs cannot progress through the DoD acquisition framework if these statutory and regulatory documents are not completed on time and of acceptable technical quality, which is determined during a complicated multi-organization review process. By providing the PM and DoD decision makers with a quantified risk assessment methodology during project planning, these key artifacts can be included in initial program risk assessment activities. This thesis provides the methodology for developing a comprehensive risk model for DoD milestone review documentation as well as recommended changes to the Capability Maturity Model Integration (CMMI) Project Planning and Risk Management process areas. The intent is to use risk as the common ground between the DoD PM and SE so that each can operate within their respective environments with a common and consistent understanding of risk.

14. SUBJECT TERMS Risk Quantification, DoD Milestone Documentation, Project Planning, Rational Frame, Political Frame, CMMI Project Planning Process Area, CMMI Risk Management Process Area, Information Support Plan (ISP)			**15. NUMBER OF PAGES** 77
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

RISK QUANTIFICATION OF SYSTEMS ENGINEERING DOCUMENTS IMPROVES PROBABILITY OF DOD PROJECT SUCCESS

Thomas C. Irwin
Director, MAGTF Command and Control, Weapons, and Sensors, Development and Integration Product Group, United States Marine Corps Systems Command
B.S., North Carolina State University, 1983

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS ENGINEERING MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 2009

Author: Thomas C. Irwin

Approved by: Walter Owen
Thesis Advisor

John Gay
Second Reader

David H. Olwell
Chairman, Department of Systems Engineering

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

A frame transition problem exists between project Systems Engineers (SE) and Department of Defense (DoD) Program Managers (PM). Systems engineering organizations, operating in a rational frame, must produce systems engineering documents required for the PM operating in a political frame of constrained resources. These artifacts, required for milestone reviews, are the results of extensive technical effort that must be accounted for and adequately resourced during project planning by the PM. Programs cannot progress through the DoD acquisition framework if these statutory and regulatory documents are not completed on time and of acceptable technical quality, which is determined during a complicated multi-organization review process. By providing the PM and DoD decision makers with a quantified risk assessment methodology during project planning, these key artifacts can be included in initial program risk assessment activities. This thesis provides the methodology for developing a comprehensive risk model for DoD milestone documentation as well as recommended changes to the Capability Maturity Model Integration (CMMI) Project Planning and Risk Management process areas. The intent is to use risk as the common ground between the DoD PM and SE so that each can operate within their respective environments with a common and consistent understanding of risk.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION....1
A. BACKGROUND....1
B. PURPOSE....3
C. RESEARCH QUESTIONS....3
D. BENEFITS OF STUDY....4
E. SCOPE AND METHODOLOGY....4

II. SYSTEMS ENGINEERING DOCUMENTATION RISK IN DOD ACQUISITION....7
A. INTRODUCTION....7
B. SYSTEMS ENGINEERING DOCUMENTATION REQUIREMENTS IN CJCSI 3170.1G, DODI 5000.2, AND CJCSI 6212.01E....7
C. ISP ROLE....12
D. RISK AREAS....14
E. SUMMARY....15

III. RESEARCH ON APPLICATION OF RISK MANAGEMENT TO SYSTEMS ENGINEERING DOCUMENTATION....17
A. INTRODUCTION....17
B. RISK MANAGEMENT, MODELING, AND ASSESSMENT....17
C. RISK MANAGEMENT OF SYSTEMS ENGINEERING DOCUMENTATION....21
D. SUMMARY....23

IV. RESEARCH ON THE HUMAN ELEMENT OF RISK MANAGEMENT....25
A. INTRODUCTION....25
B. BEHAVIORAL INFLUENCES ON RISK MANAGEMENT....25
C. ENVIRONMENTAL INFLUENCES ON RISK MANAGEMENT....30
D. SUMMARY....36

V. ISP QUANTITATIVE RISK MODEL....39
A. INTRODUCTION....39
B. ISP NETWORK DIAGRAM....40
C. PERT ANALYSIS....41
D. CRITICAL PATH ANALYSIS....43
E. ISP CUMULATIVE PROBABILITY DISTRIBUTION FUNCTION....45
F. SUMMARY....47

VI. CONCLUSION....49
A. SUMMARY OF KEY RESEARCH FINDINGS....49
B. ANSWERS TO RESEARCH QUESTIONS AND LESSONS LEARNED....50
1. Can the Risk to a Required DoD Systems Engineering Artifacts be Quantified?....50

2. Does the Quantification of Risk Support the Transition from the Rational to the Political Frame during Project Planning? 51
3. What Changes to the CMMI Project Planning Process Area should be Considered? 52
4. What Changes to the CMMI Risk Management Area Should be Considered? 53
5. Does Inclusion of Risk Quantification into Key Systems Engineering Documents during Project Planning Improve the Probability of DoD Program Success? 54
C. FUTURE RESEARCH 54
LIST OF REFERENCES 57
INITIAL DISTRIBUTION LIST 59

LIST OF FIGURES

Figure 1. Value of Systems Engineering (From: Werner Gruhl, 2004) 1
Figure 2. JCIDS and Acquisition Framework Relationship (From: CJCSI 3170.10G, March 2009) 8
Figure 3. Defense Acquisition Management System (DAMS) (From DODI 5000.02, December 2008) 9
Figure 4. JTIC Interoperability Test Process (From: CJCSI 6212.01E, December 2008) 13
Figure 5. DAMS, JCIDS, I&S Certification Relationship (From: CJCSI 6212.01E, December 2008) 14
Figure 6. Project Risk Categories (From: Forsberg, Moos, and Cotterman, 2005) 20
Figure 7. JROC Staffing Process (From: CJCSI 6212.01E, December 2008) 22
Figure 8. Systems View of Concentric Circles (From: Haimes and Schneiter, 1996) 28
Figure 9. Project Planning Process (From: (CMMI, May 2007).) 29
Figure 10. ISP Development Network (From: SSC-L Architecture COE, June 2009) 40
Figure 11. ISP Network Cumulative Probability Distribution Function 47

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1. DAMS Regulatory Documentation (From: DODI 5000.02, December 2008) 10
Table 2. Clinger Cohen Act Statutory Requirements (From: DODI 5000.02, December 2008) 11
Table 3. NR-KPP Products Matrix (From: CJCSI 6212.01E, December 2008) 12
Table 4. Four Frame Model (From: Bohlman and Deal, 1997) 32
Table 5. MCSC MC2I PG ISP Status December 18, 2008 34
Table 6. SSC-L Architecture COE Questionnaire (From: SSC-L Architecture COE, June 2009) 36
Table 7. PERT Estimates for ISP Network (From: SSC-L Architecture COE, June 2009) 43
Table 8. ISP Network Critical Path Analysis Results 44
Table 9. ISP Network Probability 46
Table 10. Changes to the CMMI Project Planning Process Area 52
Table 11. Changes to the CMMI Risk Management Area 54

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

Department of Defense (DoD) systems are acquired under Cost As an Independent Variable (CAIV) principles. The PM, who operate under this construct, in a resource constrained environment, typically react to this in the planning phase by either bypassing or partially resourcing the cost and schedule for technical activities that do not appear to tie directly to product development. These program management decisions are typically made without engineers clearly communicating the risks to the program introduced by these actions.

The result can be that key technical artifacts, required for milestone decisions, are neither of sufficient technical quality nor completed on time, thereby placing the milestone at risk. An example of a required document that is typically not fully resourced is the Information Support Plan (ISP). Fully resourced means not only the initial document creation but also the entire complex, dynamic, and iterative set of activities that are required to gain document approval are resourced by the PM.

Engineering products/activities have a better chance of being resourced if they can be represented as project risk (if X resources are not provided, then the PM must accept Y risk). The Systems Engineering process models do indeed include specific and generic practices for risk management and planning. The process models do not, however, provide a methodology for translating the engineering work into a comprehensive risk relationship (technical, program management, review process) that the PM can identify with and fund in the project planning phase. When projects are poorly planned, resources are not available, or only applied when needed, and are applied to deviations from the plan that are difficult to detect and react.

This research provides a quantitative risk methodology for DoD statutory and regulatory required technical documentation that facilitates technical and program management organization communications during the project planning phase as a means to either ensure key technical work is adequately resourced or require the PM to accept the risks. Recommended changes to the Capability Maturity Model Integrated (CMMI) risk management and project planning processes are also provided.

ACKNOWLEDGMENTS

This work would not have been possible without experiencing the Joint Executive Systems Engineering Management Program. Through Dr. Walter Owen's vision, and the faculty and staff of the Naval Postgraduate School, I have emerged two years later a better engineer, manager, and person.

Key information and discussion that led to the clarity needed to progress from idea to written word was provided by Major Chris Beckford, USMC. I am grateful for the late night emails and phone calls as well as his coordination with the SPAWAR Systems Center-LANT Architecture Center of Excellence; an outstanding group of professionals.

Brigadier General Mike Brogan, Commander Marine Corps Systems Command and Dr. John Burrow, Executive Director, never wavered in their support for me. I am extremely grateful for the opportunity they provided me, and their trust that I could accomplish this and deliver on my commitment to the men and women of the United States Marine Corps. Semper Fidelis!

Most importantly, I am grateful beyond words for the love, support, and encouragement my family has provided throughout this endeavor. I will spend the rest of my life returning it. For Lauren, Grant, and Emma, there is no prouder father than I. Someday you will understand why I did this. For my wife Gail, who shouldered the burden during this two year undertaking, you are simply extraordinary. I hope to one day be half the person you are. You are so beautiful to me.

As you, the reader, turn this page and begin your journey through this research, I begin a new chapter of service to my family and country; better for having been part of the Naval Postgraduate School, the United States Marine Corps, and better for having accomplished what I did not think was possible, but others did.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

NASA, in its "*Value of Systems Engineering; Summary report 1/04*" (Werner Gruhl, 2004), concludes that systems engineering must make up 15% of the total project estimate or the program will have overruns (Figure 1). Given that, why does the PM not simply fund the cost of a product plus 15 percent? The problem is that the SE and the PM operate in different frames (Bohlman & Deal, 1997). Engineers operate in a rational or structural frame, while the PM makes decisions in a resource constrained political frame. The PM simply cannot "fund systems engineering." A better approach is needed to tie the technical, programmatic, and organizational aspects of the program together so that the PM can make better decisions enabled from a multi-frame perspective, or enabled by providing information that can be understood in the political frame. That common ground is risk.

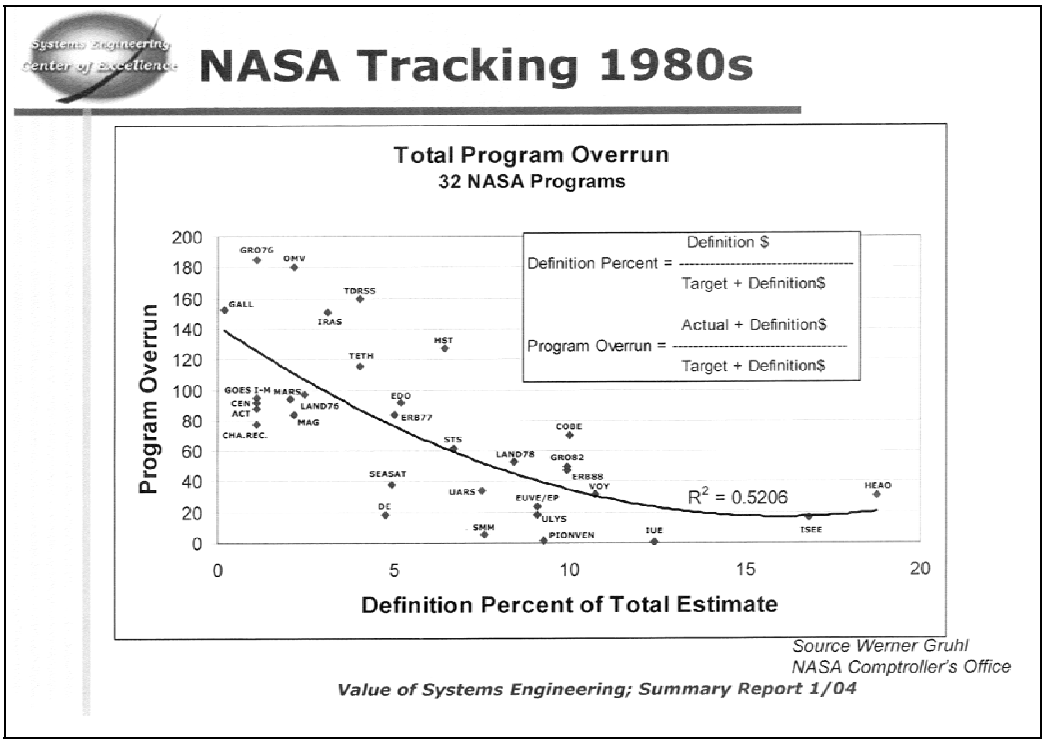

Figure 1. Value of Systems Engineering (From: Werner Gruhl, 2004)

With a view of the project dominated by the political frame, the PM either defers or partially resources technical activities that do not appear to tie directly to product development. These program management decisions are typically made because engineers do not present their cost and schedule estimates during the planning phase in terms of risk. The result can be that key technical artifacts, required by statute or regulation for milestone decisions, are neither of sufficient technical quality nor on time. Systems Engineering Plans (SEP) and Information Support Plans (ISP) are examples of statutory and regulatory required documents that are typically not fully resourced, yet necessary to decompose design and development activities to a level of detail required for successful acquisition. In this case, fully resourced means not only the initial document(s) creation but also the entire complex, dynamic, and iterative set of activities required to gain approval, execute, and manage the SEP and the ISP. The only way these and like systems engineering products/activities stand a chance of becoming fully resourced is if they can be translated from effort to project risk.

The Systems Engineering process models do indeed include specific and generic practices for risk management and planning. The process models do not, however, provide a methodology for translating the engineering work into a defined risk relationship (cost, schedule, performance) that the PM can identify with and fund in the project planning phase. When programs are poorly planned, resources are not available or applied when needed.

The Capability Maturity Model Integration (CMMI) is a process improvement maturity model for the development of products and services. The CMMI clearly identifies process improvement goals, partitions the model in process areas that are intuitive and manageable, defines process flow/relationships, and identifies the practices to be performed in each process area.

The project planning process area has three specific goals: 1) establish estimates, 2) develop a project plan, and 3) obtain commitment to plan. The typical dynamic between the PM and the SE during the estimating activities of projecting planning are a series of discussions/negotiations on “how much” engineering to fund. Estimates are integrated, with Cost As an Independent Variable (CAIV) influences, into the overall

project plan. However, because these estimates for engineering work products are not integrated into the project plan as risk, both historically and certainly those estimates are the first "CAIV victims" of the PM, putting the milestone at risk.

B. PURPOSE

This research explores the causes for under resourcing systems engineering documents required for progressing through the DoD acquisition framework. A key part of this research is to understand the reframing needed to support the PM's political decision-making process. While focusing on the ISP, this research identifies the probability of success curves for key statutory and regulatory systems engineering documentation to be considered during project planning, as well as identify changes to the CMMI project planning and risk management process areas for inclusion of risk quantification of systems engineering documents.

C. RESEARCH QUESTIONS

Systems engineering documentation, required to support system maturity assessments at milestone decisions, are artifacts that capture years of significant technical effort. With some either required by statute and/or DoD regulation, the program cannot progress through the DoD acquisition framework without them. The following questions were designed to understand the risks of under resourced systems engineering documentation on a DoD acquisition program and identify the shortfalls in the CMMI process model regarding risk quantification.

- Can the risk to a required DoD systems engineering document be quantified?
- Does the quantification of risk support the transition from the rational to the political frame during project planning?
- What changes to the CMMI Project Planning Area should be considered?
- What changes to the CMMI Risk Management Area should be considered?
- Does inclusion of risk quantification into key systems engineering documents during project planning phase improve probability of DoD program success?

D. BENEFITS OF STUDY

The combination of the complexity of DoD weapon systems and information technology (IT) systems, and the requirement (statutory and regulatory) to demonstrate program maturity at milestone review events in the acquisition framework places systems engineering documentation at the same level of importance as the system under development. The system cannot move forward through the acquisition framework, regardless of physical system maturity, without the supporting technical design documentation.

From a war-fighting perspective, needed capability cannot be delivered from the acquisition community when technical documentation, some required for certification and/or accreditation, have delayed the development and fielding process. The delay to the warfighter can also occur for the fielding of modifications or additional increments of capability to already deployed systems as they are also subjected to the DoD acquisition framework, statutory and regulatory requirements, and certification and accreditation requirements.

By providing the PM, and indirectly, the Milestone Decision Authority (MDA), with a quantified and comprehensive (technical, programmatic, and review process) risk assessment for required systems engineering documents, better decisions can be made during project planning and risk management activities. This risk model is built with the understanding and acceptance that the SE and the PM view the program from differing perspectives, driven by the environments in which they must operate. By using risk as common ground, more informed decisions can be made by both, and subsequently, a better chance of achieving project success, which must always be accepted as nothing less than delivery of capability to the warfighter.

E. SCOPE AND METHODOLOGY

This thesis will provide a comprehensive risk model for quantifying the risk of key systems engineering documentation required for DoD systems to progress through the acquisition framework as well as identify changes to the CMMI process improvement

maturity model since this process model has a history of application to DoD weapon system development. The intent is to use risk as the common ground between the DoD PM and SE so that each can operate within their respective environments with a common and consistent understanding of risk.

Both previous and current USMC ISP efforts are reviewed as well as process owner and subject matter expert interviews to understand both the existence and the severity of the problem of ISP development.

The risk model is developed around perhaps the most complex required document, the ISP. The ISP is a regulatory requirement (DODI 5000.2, December 2008) developed, matured and maintained from program initiation, through fielding and operations/sustainment. Department of Defense Architecture Framework (DODAF) architecture view development, document development, and review activities are modeled in a comprehensive network diagram with a cumulative probability distribution function (PDF) generated.

The generation of a cumulative PDF is not effective alone. Information must be supportive of the PM's decision-making process in the resource constrained political environment. To address this key human component, organization framing theory (Bohlman & Deal, 1997) is explored to understand the PM's decision-making process.

With DoD's history of applying the CMMI process improvement framework, the project planning and risk management areas of the CMMI is explored to identify areas for quantification of systems engineering documentation. By implementing changes in the CMMI, both the DoD PM and DoD industry partners can benefit.

Chapter II discusses the statutory and regulatory requirements for systems engineering documentation in DoD acquisition and their role in decision making. Next, the premise for the need to manage the risk of systems engineering documentation is set by analyzing the risk areas of the ISP.

THIS PAGE INTENTIONALLY LEFT BLANK

II. SYSTEMS ENGINEERING DOCUMENTATION RISK IN DOD ACQUISITION

A. INTRODUCTION

Systems Engineering documentation developed as part of the DoD acquisition framework (DODI 5000.2, December 2008) are artifacts that capture extensive technical work. These documents are developed and maintained throughout the acquisition lifecycle and are key parts of the decision-making process for progression through the acquisition framework. Required at milestone reviews for determining systems maturity, these documents not only require significant resources to develop, but must undergo an extensive review process through the PM, Program Executive Office (PEO), Service Acquisition Executive (SAE), Joint Staff, and Office of the Secretary of Defense (OSD) organizations prior to obtaining approval, subsequently meeting milestone entrance criteria. With these complexities and importance to program progress, risk must be managed throughout the entire development and review process.

This chapter sets the premise for the need to manage the risk of systems engineering documentation. The requirements for, and dependencies on, the ISP in the DoD acquisition framework and Chairman of the Joint Chiefs of Staff Instructions (CJCSI) are identified so that a need to manage the risk of this documentation becomes clear. The ISP is the key systems engineering artifact addressed.

B. SYSTEMS ENGINEERING DOCUMENTATION REQUIREMENTS IN CJCSI 3170.1G, DODI 5000.2, AND CJCSI 6212.01E

The war-fighting need or capability for the acquisition community to acquire a weapon system or IT system is determined through the Joint Capabilities Integration Development System (JCIDS) process as directed in Chairman of the Joint Chiefs of Staff (CJCS) policy (CJCSI 3170.10G, March 2009). Figure 2, from CJCSI 3170.10G, shows the relationship established by this joint policy, between the JCIDS process and the DoD acquisition framework. Requirements documentation, born from a joint

Capabilities Based Assessment (CBA), is refined as the material solution matures. The Initial Capabilities Document (ICD) drives the first acquisition decision, the Material Development Decision (MDD), where the Milestone Decision Authority (MDA) authorizes entry into the Defense Acquisition Management System (DAMS). As the material solution matures, the requirements documents also mature as do the Capabilities Development Document (CDD), driving the Engineering and Manufacturing Development (EDM) phase, and the Capabilities Production Document (CPD), driving the Production and Deployment phase.

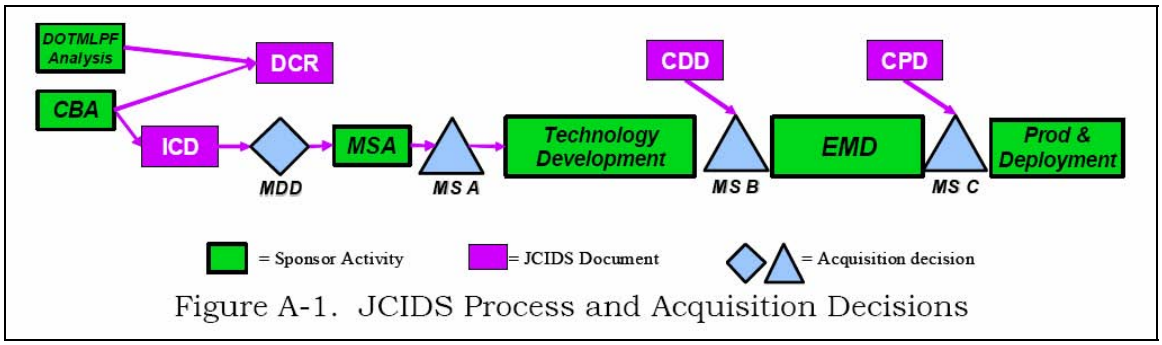

Figure 2. JCIDS and Acquisition Framework Relationship (From: CJCSI 3170.10G, March 2009)

The ISP, a key systems engineering document, is a requirement of the Net Ready Key Performance Parameter (NR-KPP) (CJCSI 6212.01E, December 2008). Per the CJCS 3170.01G JCIDS policy, the KPPs are validated at CDD approval. Therefore, key systems engineering documents can also introduce risk into the requirements maturation process, which must remain in synchronization with the acquisition management process.

DODI 5000.02, December 2008 establishes a simplified and flexible management framework for translating capability needs and technology opportunities, based on approved capability needs, into stable, affordable, and well-managed acquisition programs that include weapon systems, services, and Automated Information Systems (AISs) (DODI 5000.02, December 2008). The Defense Acquisition Management System

(DAMS), Figure 3, from DODI 5000.02, December 2008 has decision points where both requirements and technical maturity are assessed as defined in the milestone entrance and entry criteria.

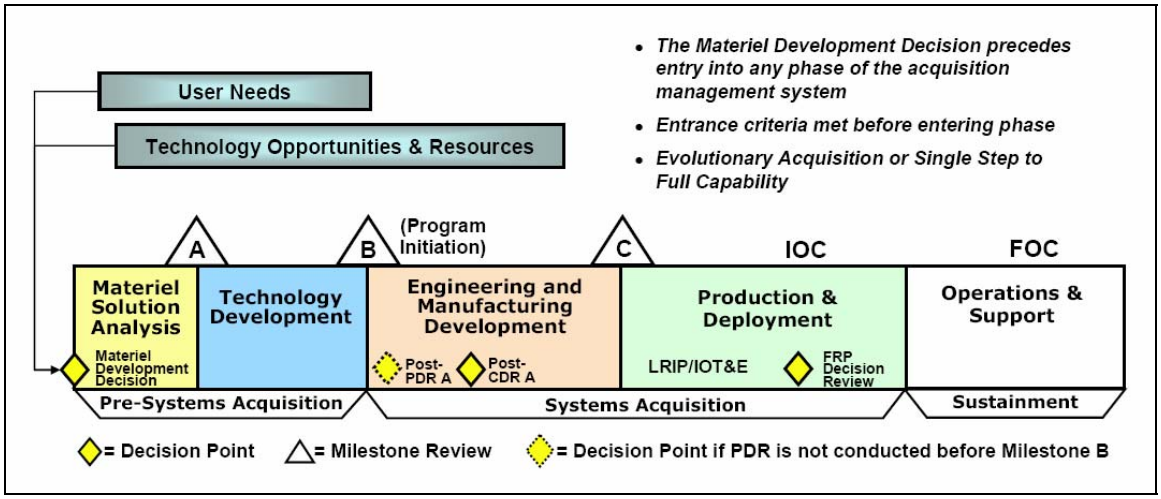

Figure 3. Defense Acquisition Management System (DAMS) (From DODI 5000.02, December 2008)

Table 1 is an excerpt from Table 3 of DODI 5000.02, which lists the regulatory requirements for each milestone. Systems engineering documentation required for these milestones can be found in that table. This excerpt was chosen to highlight the ISP requirement. The ISP is also a statutory requirement of the Clinger Cohen Act (CCA), Table 2 (DODI 5000.02, December 2008). In addition to the ISP, the Systems Engineering Plan (SEP) and the Test and Evaluation Master Plan (TEMP) are examples of other systems engineering documents required for milestone decisions. Each of those documents, in addition to the significant resources required for development, have a lengthy multi-organizational review and approval process that must be complete to support a milestone decision. Even with the technical complexity, the ISP is also subjected to complex and independent statutory, regulatory, and JCIDS review processes. Without proactive and frequent involvement with the reviewing and approving organizations, the document may be delayed.

Cost Analysis Requirements Description (CARD) (MDAPs and MAIS acquisition programs only) (CARDs shall be prepared according to the procedures specified in Enclosure 7 of this Instruction)	This Instruction	For MDAPs - Program Initiation for Ships - MS B - MS C - Full-Rate Production DR For MAIS - Any time an Economic Analysis is required–either by statute or by the MDA
Corrosion Prevention Control Plan (part of Acquisition Strategy) (ACAT I only)	DoDI 5000.67 (Reference (aj)) This Instruction	MS B MS C
CPD	Reference (h)	MS C
Defense Acquisition Executive Summary (MDAPs and MAIS only)	This Instruction	Quarterly Upon POM or BES submission Upon unit cost breach
DoD Component Cost Estimate (mandatory for MAIS; as required by CAE for MDAP)	This Instruction	MS A For MDAPs - Program Initiation for Ships - MS B - Full-Rate Production DR For MAIS - Any time an Economic Analysis is required–either by statute or by the MDA
Exit Criteria	This Instruction	Program Initiation for Ships MS A MS B MS C Each Review
ICD	Reference (h)	Materiel Development Decision MS A MS B MS C (if Program Initiation)
Independent Technology Readiness Assessment (ACAT ID only) (if required by the office of the Director, Defense Research and Engineering)	This Instruction	MS B MS C
Information Support Plan (ISP) (All IT–including NSS)	DoD Directive 4630.05 (Reference (ak)) DoD Instruction 4630.8 (Reference (al))	Program Initiation for Ships (Initial ISP) MS B (Initial ISP) CDR (Revised ISP) (unless waived) MS C (ISP of Record)
IT and NSS Joint Interoperability Test Certification (All IT–including NSS)	Chairman of the Joint Chiefs of Staff Manual 3170.01 (Reference (am)) CJCSI 6212.01 (Reference (an)) Reference (ak)	Full-Rate Production DR (or Full Deployment DR)
IUID Implementation Plan	DoD Instruction 8320.04 (Reference (ao))	MS A (summarized in SEP) MS B (annex to SEP) MS C (annex to SEP)
LCSP (part of Acquisition Strategy)	This Instruction	MS B MS C Full-Rate Production DR
Life-Cycle Signature Support Plan	DoD Directive 5250.01 (Reference (ap))	MS A (summarized in TDS) Program Initiation for Ships MS B MS C (updated as necessary)

Table 1. DAMS Regulatory Documentation (From: DODI 5000.02, December 2008)

Actions Required to Comply With Subtitle III/CCA (Reference (v))	Applicable Program Documentation[1]
1. Make a determination that the acquisition supports core, priority functions of the Department. [2]	ICD Approval
2. Establish outcome-based performance measures linked to strategic goals. [2, 3]	ICD, CDD, CPD and APB approval
3. Redesign the processes that the system supports to reduce costs, improve effectiveness and maximize the use of COTS technology. [2, 3]	Approval of the ICD, Concept of Operations, AoA, CDD, and CPD
4. Determine that no Private Sector or Government source can better support the function. [4]	Acquisition Strategy page XX, para XX AoA page XX
5. Conduct an analysis of alternatives. [3, 4]	AoA
6. Conduct an economic analysis that includes a calculation of the return on investment; or for non-AIS programs, conduct a Life-Cycle Cost Estimate (LCCE). [3, 4]	Program LCCE Program Economic Analysis for MAIS
7. Develop clearly established measures and accountability for program progress.	Acquisition Strategy page XX APB
8. Ensure that the acquisition is consistent with the Global Information Grid policies and architecture, to include relevant standards.	APB (Net-Ready KPP) ISP (Information Exchange Requirements)
9. Ensure that the program has an information assurance strategy that is consistent with DoD policies, standards and architectures, to include relevant standards. [3]	Acquisition Information Assurance Strategy
10. Ensure, to the maximum extent practicable, (1) modular contracting has been used, and (2) the program is being implemented in phased, successive increments, each of which meets part of the mission need and delivers measurable benefit, independent of future increments.	Acquisition Strategy page XX
11. Register Mission-Critical and Mission-Essential systems with the DoD CIO. [3, 5]	DoD IT Portfolio Repository

1. The system documents/information cited are examples of the most likely but not the only references for the required information. If other references are more appropriate, they may be used in addition to or instead of those cited. Include page(s) and paragraph(s), where appropriate.

2. These requirements are presumed to be satisfied for Weapons Systems with embedded IT and for Command and Control Systems that are not themselves IT systems.

3. These actions are also required to comply with section 811 of Reference (ag).

4. For NSS, these requirements apply to the extent practicable (section 11103 of Reference (v))

5. Definitions:

Mission-Critical Information System. A system that meets the definitions of "information system" and "national security system" in the CCA (Reference (v)), the loss of which would cause the stoppage of warfighter operations or direct mission support of warfighter operations. (The designation of mission critical shall be made by a Component Head, a Combatant Commander, or their designee. A financial management IT system shall be considered a mission-critical IT system as defined by the Under Secretary of Defense (Comptroller) (USD(C)).) A "Mission-Critical Information Technology System" has the same meaning as a "Mission-Critical Information System."

Mission-Essential Information System. A system that meets the definition of "information system" in Reference (v), that the acquiring Component Head or designee determines is basic and necessary for the accomplishment of the organizational mission. (The designation of mission-essential shall be made by a Component Head, a Combatant Commander, or their designee. A financial management IT system shall be considered a mission-essential IT system as defined by the USD(C).) A "Mission-Essential Information Technology System" has the same meaning as a "Mission-Essential Information System."

Table 2. Clinger Cohen Act Statutory Requirements (From: DODI 5000.02, December 2008)

The ISP is also required to support the Interoperability and Security (I&S) certification requirements of CJCSI 6212.01E. As an example of the complexities in the review process alone mandated in CJCSI 6212.01E Enclosure D (December 2008, p. D-1), Joint Staffing and Certification Process, the following excerpt is provided:

> CDD/CPD NR-KPP Technical Artifacts shall reside in the corresponding ISP and be readily available to all reviewers at the time of the CDD/CPD review (i.e., be included as an attachment or referenced as a hyperlink within the CDD/CPD). The use of the Enhanced Information Support Plan (EISP) tool is encouraged to facilitate the development of a standard ISP format and assist programs in risk mitigation. (CJCSI 6212.01E Enclosure D (December 2008, p. D-1) Joint Staffing and Certification Process)

Note, this is the first time risk is mentioned in policy or instruction with this document, and there is no mention of risk in DODI 5000.02 (December 2008).

C. ISP ROLE

The ISP is not only a key systems engineering document capturing all but one of the required DODAF Enterprise Architecture Products (Table 3), but is also a statutory and regulatory requirement for DoD National Security Systems (NSS) and information technology (IT) systems as well as a required document for I&S certification (CJCSI 6212.01E, December 2008).

Document	Supportability Compliance	DOD Enterprise Architecture Products (IAW DODAF) (see Note 5)																Data/Service Exposure Sheets	IA Compliance	GTG Compliance
		AV-1 /AV-2	OV-1	OV-2	OV-3	OV-4	OV-5	OV-6C	OV-7	SV-1	SV-2	SV-4	SV-5	SV-6	SV-11	TV-1	TV-2			
ICD			X																	
CDD	X	3	X	X	X	X	X	X			X	X	X	X		2	2	1	X	X
CPD	X	3	X	X	X	X	X	X	1		X	X	X	X	1	2	2	1	X	X
ISP	X	3	X	X	X	X	X	X	4		X	X	X	X	4	2	2	1	X	X
TISP	X	3	X		X		X	X		X			X	X		2	2	1	X	X
ISP Annex (Svcs/ Apps)	X	3	X				X				X	X	X	X		2	2	1	X	X
X		Required (PM needs to check with their Component for any additional architectural/regulatory requirements for CDDs, CPDs, ISPs/TISPs. (e.g., HQDA requires the SV-10c)																		
Note 1		Required only when IT and NSS collects, processes, or uses any shared data or when IT and NSS exposes, consumes or implements shared services,																		
Note 2		The TV-1 and TV-2 are built using the DISRonline and must be posted for compliance.																		
Note 3		The AV-1 must be uploaded onto DARS and must be registered in DARS for compliance																		
Note 4		Only required for Milestone C, if applicable (see Note 1)																		
Note 5		The naming of the architecture views is expected to change with the release of DODAF v2.0 (e.g., StdV, SvcV, StdV, DIV). The requirements of this matrix will not change.																		

Table E-1. NR-KPP Products Matrix

Table 3. NR-KPP Products Matrix (From: CJCSI 6212.01E, December 2008)

The ISP is also a critical part of the Joint Interoperability Test Command (JITC) Interoperability Test and Certification Process as shown in Figure 4. The ISP, as one of the five elements of the Net Ready KPP (NR-KPP), drives the testing planning, execution, and assessment. The assessment leads to the JITC I&S certification needed for progression through Defense Acquisition Management System (DAMS) and fielding. With an approved ISP required for the Interoperability and Supportability (I&S) certification, the technical resources (funded by the PM) must be provided or the ISP is at significant risk of being approved, subsequently placing the system under development at risk of being fielded and sustained.

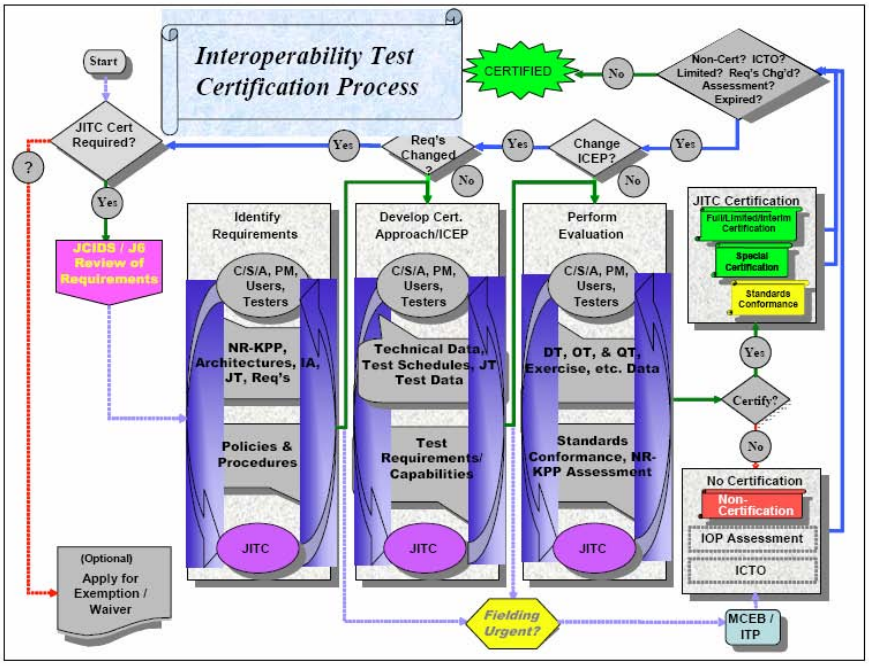

Figure F-1 Joint Interoperability Test Certification Process

Legend:			
Cert	Certification	JT	Joint Threads
DT	Developmental Test	MCEB/ITP	Military Communications-Electronics Board/Interoperability Test Panel
IA	Information Assurance	NR	Net-Ready
ICEP	IOP Certification Evaluation Plan	NR-KPP	Net-Ready Key Performance Parameter
IOP	Interoperability	OT	Operational Test
ICTO	Interim Certificate to Operate	PM	Program Manager (Sponsor)
JCIDS	Joint Capabilities Integration and Development System	QT	Qualification Test
JITC	Joint Interoperability Test Command	Req's	Requirements
J-6	Joint Staff J-6	Std's	Standards Conformance

Figure 4. JTIC Interoperability Test Process (From: CJCSI 6212.01E, December 2008)

D. RISK AREAS

Figure 5 provides a visualization of the complexities for the ISP to support the DAMS, JCIDS, and I&S certification. There are three separate but related processes executing simultaneously. Each process has a multi-organizational oversight and review processes that, with a failure (either in review schedule, or technical issues) in one process, cascades into the next.

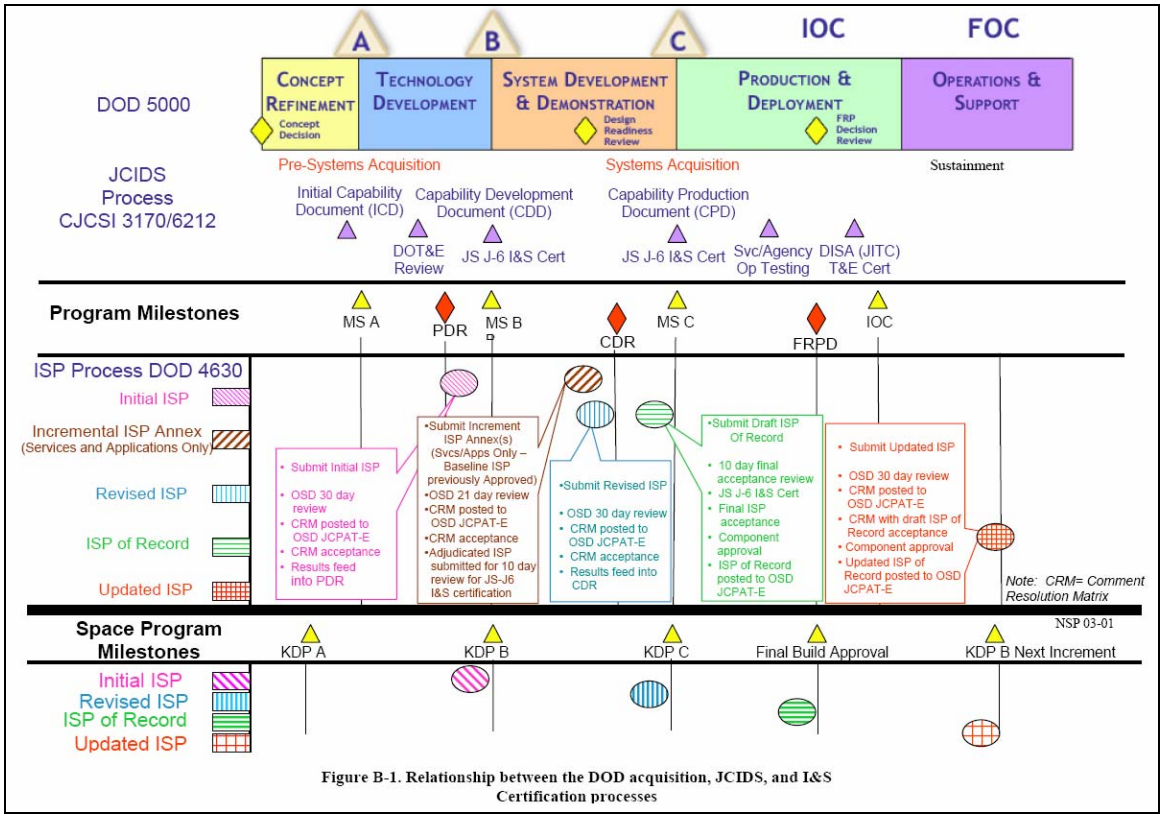

Figure B-1. Relationship between the DOD acquisition, JCIDS, and I&S Certification processes

Figure 5. DAMS, JCIDS, I&S Certification Relationship (From: CJCSI 6212.01E, December 2008)

The technical complexity of the ISP and the complexity of the review process introduce risk to progression through each of the three processes. Technical risk resides in the DODAF Integrated Architecture Products and schedule risk in the review and certification processes. Finally, cost risk resides in the rework and certification retest.

E. SUMMARY

Systems engineering documentation is required, both by statutory law and regulatory policy, at the Joint, Agency, and Service acquisition levels. As such, these technical artifacts are as important as the technical maturation of the system itself. This chapter examined the specific case of the ISP because of the criticality of the document and the complexity of technical content and review process. Without these artifacts being technically sound and reviews/approvals complete, system progression through the DoD acquisition framework does not occur. Applying risk management practices specifically to these documents, as part of the initial project planning, is therefore warranted. The only instance where the ISP is mentioned as a tool for risk management is in CJCSI 6212.01E. There is no mention in DODI 5000.2 that technical artifacts like the ISP should be connected to risk management. Given the information provided in this chapter, risk management practices should be targeted specifically at systems engineering documentation.

With the premise set that there is indeed a need to manage the risks to systems engineering documents, Chapter III furthers research risk management, risk modeling, and risk assessment as key tenants of controlling uncertainty in the development, review, and approval of these technical artifacts.

THIS PAGE INTENTIONALLY LEFT BLANK

III. RESEARCH ON APPLICATION OF RISK MANAGEMENT TO SYSTEMS ENGINEERING DOCUMENTATION

A. INTRODUCTION

Although risk management principles are required for all Major Defense Acquisition Programs (MDAP), effective implementation of risk management is more difficult and less likely. Of 25 MDAP programs examined by GAO, only three had adequately performed the five criteria essential for assessing technical risk (E. H. Conrow, 2003). The management of project risks, typically around cost, schedule, and performance is a requirement for the DoD PM. Both quantitative and qualitative approaches are applied as deemed appropriate by the PM. In fact, the PM is more likely to be risk averse than be proactive risk managers because of the additional oversight, attention, and reporting that the identification of risk brings to today's DoD programs.

This chapter researches risk management, risk modeling, and risk assessment, and explore applicability to systems engineering documentation as a tenant of controlling uncertainty in the development, review, and approval of these technical artifacts. Chapter IV then examines the human element of risk management. Since Program Management and the development of complex warfighting systems is a human endeavor, it is necessary to understand the effect of human behavior and perspective on risk management.

B. RISK MANAGEMENT, MODELING, AND ASSESSMENT

The complexity of modern weapon systems and IT systems introduces inherent uncertainties in the cost, schedule, and performance of the program, which will eventually deliver them to the warfighter. These uncertainties make it essential that proactive risk management occur.

There are common themes, or tenants, of an effective risk management program. First and foremost, is that although risk management is an integral part of the project, it must be addressed specifically (Y. Y. Haimes, 2004). Therefore, risk management plans,

risk management boards, and risk specific processes for identification, modeling, classification, mitigation, control, and assessment are part of an effective risk strategy. Risk management is also a continuous effort that lasts throughout the project since risks can be introduced at all phases. Factors such as shortages in commercial commodities, introduction of new commercial technologies, funding cuts, and requirements changes can occur at anytime. The implementation of a sound risk management approach can address these uncertainties.

Risk management is essential because key cost, schedule, and performance attributes are uncertain or unknown until late in the program. However, risks can be identified early in the program and alleviated with good risk management practices. Further, risk management should be considered as part of the day-to-day job function at the working level (Conrow, 2003).

With risk management touching all phases, aspects, and organizations associated with a project, clear roles and responsibilities for risk management are required. E. H. Conrow (2003) recommends that a Risk Manager be assigned and that a Risk Management Board (RMB) is formed, chaired by the PM. The RMB is the hub of the risk management effort, is inclusive of engineers and project managers, and performs the following (Conrow, 2003, p. 116).

- Prioritizes risks
- Defines risk management roles and responsibilities
- Works all risk issues.
- Makes or concurs with all risk management related decisions

With engineers and project managers participating in the RMB, and with all risk issues worked and documented in that forum, it is important that representatives of the different elements of the project are able to communicate the risks in their areas of responsibility. Although the human element of risk management is addressed in Chapter IV, the point here is that critical decisions affecting project success are made in a board setting requiring effective communications.

Maintaining perspective on the problem at hand is an important part of program management. Therefore, it is important to define both risk and risk management in the context of the project since it is ultimately the project that needs to be successful for the war-fighting capability to be fielded. Smith and Merritt (2002, p. 5) define risk "as the possibility that an undesired outcome-or the absence of a desired outcome-disrupts your project" and risk management as "the activity of identifying and controlling undesired project outcomes proactively." There are many definitions of risk and risk management. Smith and Merritt's (2002) definition of risk was not chosen for convenience, but for the direct relationship between risk and the project. For DoD acquisition, it is the entire project that must succeed; the system must work (effective and suitable), statutory and regulatory requirements met, mandated process and policies followed, milestone decisions approved, certifications and approvals obtained. Therefore, risk must be managed in the context of the project, not just the cost, schedule, and performance of the weapon, or IT system, specifically.

Forsberg, Moos, and Cotterman (2005), provide visualization for whether risks must be managed from a project perspective (Figure 6). System performance is not enough for the program to be successful. External and internal implementation risks can lead to the project's cancellation, regardless of system performance and maturity (Forsberg, Moos, and Cotterman, 2005). With the political environment in which DoD systems are acquired, programs are particularly vulnerable to implementation risks (funding, political support, resources). Of particular note is the identification of planning as an internal risk. Statutory and regulatory systems engineering documentation must be accounted for in proper project planning. With the technical and review/approval complexities of these documents, the uncertainties must be addressed with risk management. In fact, the CMMI includes risk management in the Project Management Process Area (CMMI, May 2007).

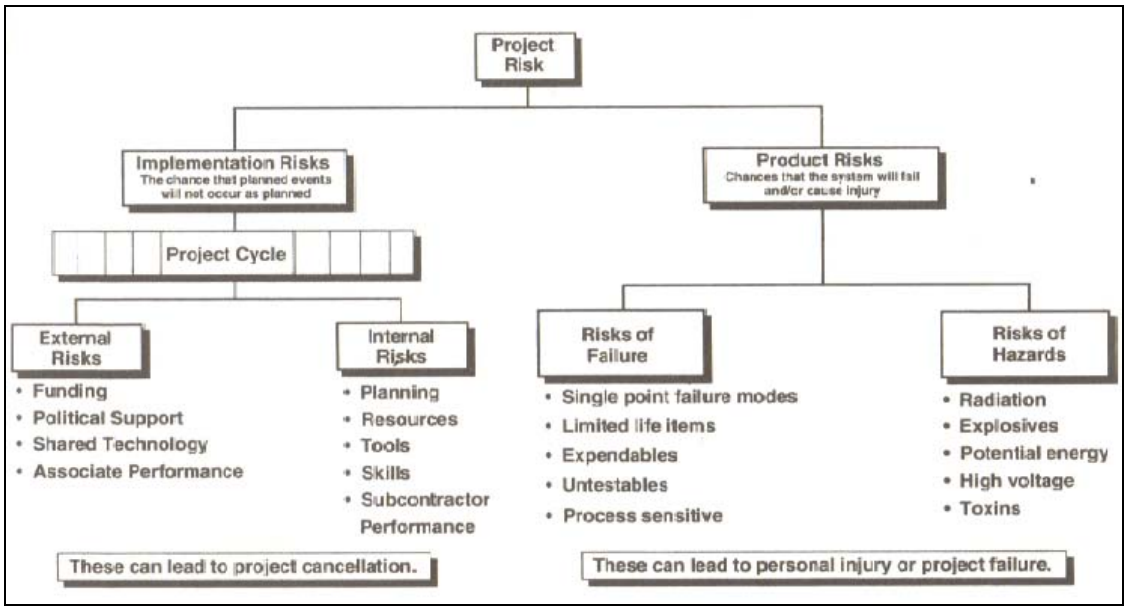

Figure 6. Project Risk Categories (From: Forsberg, Moos, and Cotterman, 2005)

Accurate assessment of risks is an essential step in implementing effective risk mitigation strategies as part of the overarching risk management strategy. Both qualitative and quantitative methods can be applied. Qualitative analysis uses judgment and expert opinion to evaluate the probability and consequence values, where quantitative analysis uses probabilistic and statistical methods (Ayyub, 2003).

The choice to use either qualitative or quantitative methods is largely determined by the quality and availability of data. Without detailed data, qualitative analysis can still be performed and be founded on subject matter experts' opinions and judgments. Although perhaps not optimal, risk mitigation plans can still be generated and the RMB can still manage all the risks. Additionally, the identified risk may not be serious enough to warrant expenditure of project resources to model and quantitatively assess the risk. It simply may not be needed.

Quantitative risk analysis distills risk down into a numeric probability or likelihood of failure. For the purposes of this research, the inverse is applied to quantify the probability of success of having critical systems engineering documentation approved as required for milestone decisions and fielding of capability. Equally as important, "quantitative analysis generally provides a more uniform understanding among different

individuals, but requires quality data for accurate results" (Ayyub, 2003, p. 84). Too often, the different perspectives and competition for resources lead to an inability to find common ground resulting in inaccurate assessments of risk. With project risks quantified, the diverse project team's energy and resources can be directed toward a common understanding of those things that could cause project failure.

To generate the quantitative probability distribution functions, the system and/or processes must be modeled before analysis can begin. Event Modeling (Event Trees, Success Trees, and Fault Trees) are systemic and often the most complete way to identify accident scenarios and quantify risk (Ayyub, 2003). Event trees identify failures from an initiating event and are further refined by modeling only the significant successes and failures through Success Tree and Fault Tree analysis. The outcome of the Success and Fault Tree analysis is the probability of occurrence of the top-level event, whether it is a top-level success or failure.

Network modeling, particularly from a project management perspective, can be an effective method for quantitative risk analysis. DoD acquisition programs are typically, large projects with many interrelated activities, and must be executed in a specific time sequence (milestone decisions). By representing the project, and sub-projects as a network(s), the probability of network success can be quantified. A network is a set of nodes connected in various ways by directional arcs (Ragsdale, 2007). Since DoD programs operate within a specific framework (DODI 5000.02, December 2008), and particularly with industry demonstrating process discipline (CMMI, 2007), task times and nodes can be accurately defined. The opportunity to apply network modeling effectively to project management is certainly there and explored in Chapter V.

C. RISK MANAGEMENT OF SYSTEMS ENGINEERING DOCUMENTATION

The complexity of the review and approval process alone for statutory and regulatory required systems engineering documents, introduces uncertainties that must be managed as risk. To make the point, Figure 7 shows the JROC review process for documentation and provides a good visualization of the complexity of only one part of

the review process. Each of these organizational reviews introduces uncertainties, particularly in that they are resource constrained introducing a queuing problem as well.

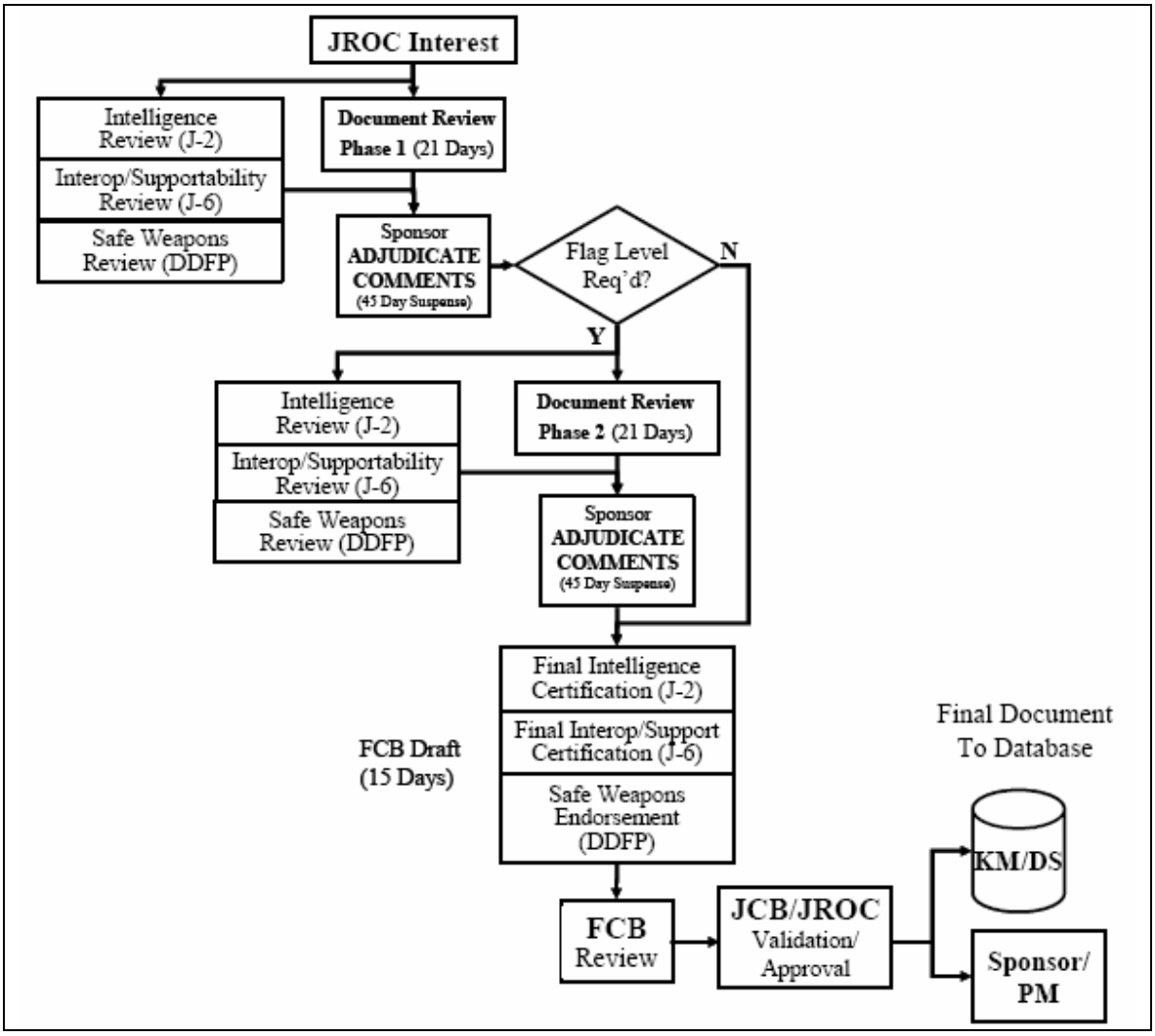

Figure 7. JROC Staffing Process (From: CJCSI 6212.01E, December 2008)

The JROC staffing process is preceded by a thorough local organizational review and Service level review that is no less complex, and therefore, introducing uncertainties and risk. All of the review processes must be complete before the program can move forward.

In addition to the review and approval processes, systems engineering documents must be built in a specific sequence or extensive rework and inefficient application of resources results affecting both cost and schedule. For example, 90% of the required information in a Systems View-6 (SV-6) of the CDD and ISP is a paste from the Operational View-3 (OV-3). Operational Views (OV) are architecture views describing the joint capabilities as well as identifying the operational nodes and critical information needed (CJCSI 6212.01E, December 2008). The OV-3 is therefore built by the requirements organization, not the acquisition organizations. The building of each of these views is dependent on information from other views as well as information from other interoperating organizations. Until the OV-3 is complete, for example, the SV-6 cannot be completed. Uncertainty is introduced simply from the dependencies and given the complexity of interoperability between systems. Uncertainty is also introduced from the technical challenges of data and information exchange between war-fighting systems. The criticality of these systems engineering documents to the project along with the uncertainties introduced through the complex technical challenges of interoperability and the multiple review processes clearly warrant a specific risk management effort.

D. SUMMARY

Having explored the need, and in fact the requirement, for DoD programs to manage project uncertainty through the implementation of sound and proactive risk management strategies, research has yet to find systems engineering documentation specifically addressed as a risk or the need to manage it. These documents are statutory and/or regulatory requirements for DoD weapon, and IT systems to progress through the acquisition process, including operations and sustainment. Furthermore, these documents are technical artifacts capturing significant technical effort that drive system design and through the review and approval process, demonstrate technical maturity required for milestone decisions.

With the addition of the complex multi-organizational review and approval process, the uncertainties must be specifically addressed through risk management, driven by quantitative risk analysis. The sequential nature of the development and review of these technical artifacts lends itself to the application of network modeling to quantify the probability of failure, and inversely, the probability of success, that these documents are ready on time to support the DoD acquisition process.

The acceptance that controlling the uncertainty of the project must include risk management of systems engineering documentation is a key acknowledgement by a PM. However, even when acceptance is combined with motivation and commitment to manage risk, effective risk management requires and understanding of the human decision making process. It is, therefore, necessary to explore the human element of risk management in the next chapter.

IV. RESEARCH ON THE HUMAN ELEMENT OF RISK MANAGEMENT

A. INTRODUCTION

The establishment of Risk Management Boards, the inclusion of all project team members in risk management, qualitative and quantitative assessment of project risks, and the complex review and approval processes for systems engineering documents bring human and environmental influences inherent in the diverse nature of the work and the contributing organizations. Each organization has a perspective and culture that affects results, each has responsibility and/or accountability for the quality and timeliness of critical project needs, and each has external influences not controlled by the project.

This chapter explores the human element in risk management. Project data is analyzed, severity and impact assessed, and mitigation plans established. However, organizations and individuals can look at the same data and arrive at different conclusions. This not only occurs inside project teams, but in every day lives. For example, a jury sees the same data, but arrives at different conclusions. The same goes for voting, political party loyalty and even brand loyalty. With the human influence on results and conclusions, application of the research into the human element of risk management is essential for developing an accurate risk model and quantitative assessment method defined in Chapter V.

B. BEHAVIORAL INFLUENCES ON RISK MANAGEMENT

Both individual and organizational behaviors impact the ability to implement an effective risk management program. “Social learning theory, as proposed by Albert Bandura, encompasses a theory of observational learning that holds most people learn behaviors by observing others and then modeling the behaviors perceived as being effective” (Wagner & Hollenbeck, 1992, p. 109). For example, if a project engineer disagrees with a technical solution proposed by management and is summarily chastised or punished, it is then more than likely that bad news is not brought forward again.

Furthermore, if management's reaction is seen as effective or appropriate by others, then any other technical disagreements may not be brought forward. Risk management, to be effective, has to be implemented at the lowest levels of the project team. With that, organizational leaders must encourage the responsible identification and proactive management of risk by all.

Risk management must be performed commensurate with holistic systems engineering and systems thinking. Risks cannot be identified and managed in a sporadic or ad-hoc fashion or critical program risks may never be mitigated. "Good management of technological systems must address the holistic nature of the system in terms of its hierarchical, organizational, and fundamental decision making structure" (Haimes, 2004, p. 18). In this statement, Haimes points directly at the human element aspect of effective risk management. Implementation must be dovetailed into the project team's normal operations so that risk management occurs at the lowest levels, and is allowed to execute like other team work and reporting. However, large projects have many teams, cultures, and operations processes that contribute to inefficiencies and errors in communications and integration of team functions. The quantification of risks from an end-to-end product development viewpoint provides common ground for the right organizational dynamics and decision making to unfold. The comprehensive network model and resulting cumulative probability function upcoming in Chapter V provides the approach for bridging organizational and perspective divides by offering a single cumulative distribution function for the technical, review, and approval functions.

Haimes (2004) takes the idea that the holistic or systems thinking needed for project success can be realized by building on Covey's principles of personal leadership in the book "*The Seven Habits of Highly Effective People*" (Covey, 1989). "Indeed, Covey's journey for personal development as detailed in his book has much in common with the holistic systems concept that constitutes the foundation of the field of systems engineering" (Haimes, 2004, p. 5). Covey (1989) promotes the following seven habits.

Habit 1	Be proactive
Habit 2	Begin with the end in mind
Habit 3	Put first things first
Habit 4	Think win-win
Habit 5	Seek first to understand, then to be understood
Habit 6	Synergize
Habit 7	Sharpen the saw

With the focus of this research on the introduction of a comprehensive quantitative risk model in the project planning phase, Habit 1 and Habit 2 will be explored because they are key personal behaviors that affect the project team's ability to plan the project, including planning for uncertainties.

Being proactive (Habit 1) addresses how to view the problem. Covey approaches the problem with a concept of concentric circles. The Circle of Concern includes all things that are important while the Circle of Influence includes those things that are not under the project team's control (Haimes, 2004). It is imperative that the project team embrace this; particularly, since the review/approval and certification activities of key systems engineering documents occurs outside of the project team's circle of influence. It is not enough to manage the uncertainty of the internal technical work, since the project is still at risk of failure due to the uncertainties in the extensive complex review and approval processes discussed earlier. The accomplishment of technical work cannot be severed from the review, approval, and certification process. The project network proposed for the ISP in Chapter V encompasses both of Covey's circles by accounting for the end-to-end, or comprehensive, effort required to obtain ISP approval.

There are two key tenants of Habit 2; begin with the end in mind. The first is to begin with the image of the end. Covery (1989) states, "To begin with the end in mind means to start with a clear understanding of your destination. It means to know where you're going so that you better understand where you are now and so that the steps you take are always in the right direction" (p. 98). Figure 8 (Haimes and Schneiter, 1996)

provides a visualization of the holistic view of the things that can be influenced, those that cannot, and the uncertainties and realities a project team must address to reach the end.

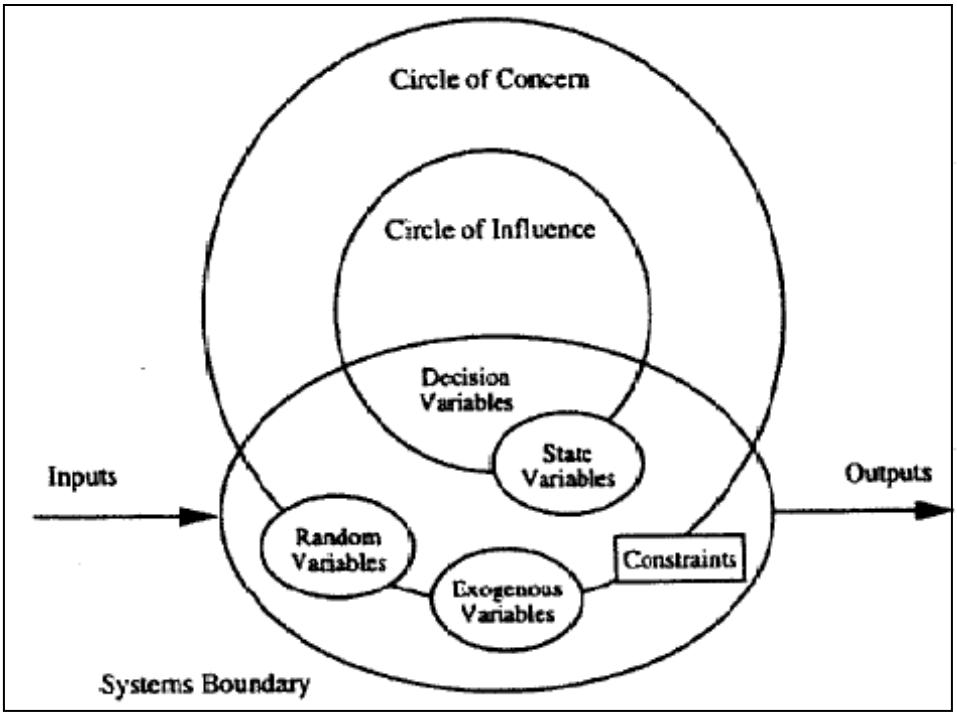

Figure 8. Systems View of Concentric Circles (From: Haimes and Schneiter, 1996)

To relate this to project management, the performance of project planning per the CMMI Project Planning Process Area (Figure 9) is the means by which the project team "begins with the end in mind." The Specific Goal (SG) 1 forms the image of the end by defining the scope and life cycle of the project while (what is it, and how long does it live) while Specific Practice (SP) 2.1 identifies the uncertainties in the steps to be taken toward the end state (CMMI, May 2007).

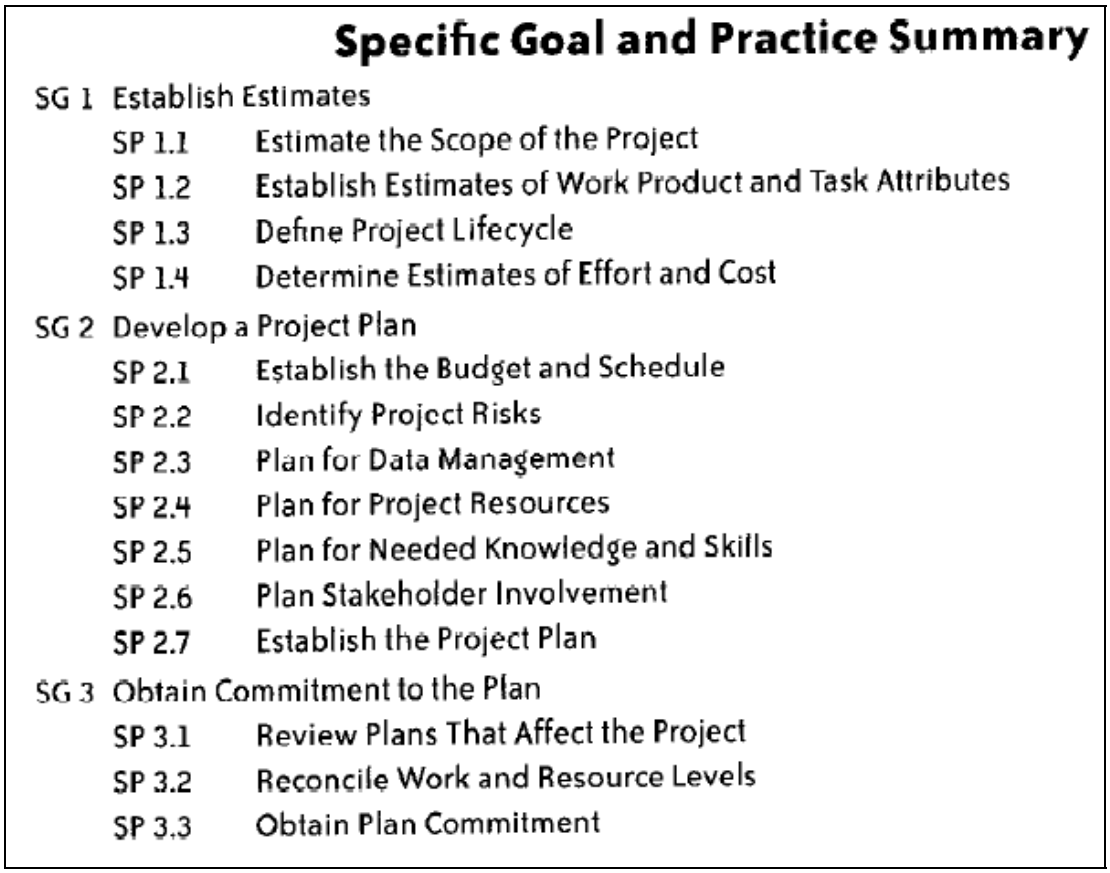

Figure 9. Project Planning Process (From: (CMMI, May 2007).)

The second tenant is:

> All things are created twice. Take the construction of a home, for example. You create it in every detail before you ever hammer the first nail into place…….you work with ideas. You work with your mind until you get a clear image of what you want to build. Then you reduce it to blueprint and develop construction plans…….Then in the second creation, the physical creation, you will have to make expensive changes that may double the cost of your home……you begin with the end in mind. (Covey, 1998, p. 99)

Covey indicates that things must be built twice; the latter being the physical object that can be executed in project planning activities, followed by development of the physical system. For DoD programs, more than the physical system must be built both times. With the mandate to meet statutory and regulatory requirements during acquisition, those key systems engineering documents must also be built twice. As

previously addressed, the program cannot be successful if both the technical quality and time elements (milestone reviews) of these documents are not planned for, i.e., the first build, and then delivered, i.e., the physical build.

It is essential for the project success that at the beginning (project planning), the PM has a clear image that the end of a successful program include the following.

- Delivery of an effective, suitable, and affordable system
- Delivery of a system on time
- Delivery of systems engineering documentation that is in compliance with all statutory and regulatory requirements

Experience has shown that the PM is typically shortsighted with item 3. In other words, the maturity of the systems engineering documentation becomes an increasing concern as the milestone approaches. It is almost certainly not planned for at the beginning, with the same detail and energy as the system development work is planned for, to include risk. The comprehensive quantitative risk model proposed in Chapter V begins the systems engineering documentation work with the end in mind. For the ISP, the end must be an approved document, which is not always in the circle of influence. Failure to have this document approved, within the time sequence the program needs, results in program failure.

C. ENVIRONMENTAL INFLUENCES ON RISK MANAGEMENT

In addition to the influence of human behaviors on the success or failure of a project, the environments in which the SE and PM operate in affect perspective, behaviors, and actions. Haimes (2004, p. 7) states:

> Covey stresses the understanding of paradigms–the lenses through which we see the universe. Furthermore….it is not what happens to us that affects our behavior; rather, it is our interpretation of what happens. Since our interpretation of the world we live in determines how we create new and innovative solutions to the problems we face…understanding the systemic nature of the universe and defining the system that we need to address are imperative requirements for our ability to solve problems.

The PM and SE see the world through different lenses. The PM is responsible and accountable for the overall success or failure of the program. Managing cost, schedule, performance, constraints, stakeholder relationships, oversight relationships, contracts, CAIV, T&E, reporting requirements, and endless briefings consume the PM's time and attention. It is a politically charged environment where competition for resources, hidden and secondary agendas, and inquiries from powerful DoD and congressional leaders must be navigated through so that the project team can execute.

Systems Engineers see the world as more structured. Rational and logical thought processes are dominate for problem solving and decision making; start with the requirements, develop functional, allocated, and physical baselines, architect and design, build and test, etc. The technical problems are no less complex than the PM. Just different: requiring a different mindset and approach for success.

The different lenses through which these two entities of the project team see the world cause communication issues, which start at the very beginning of the project, during planning when resources are estimated. How do the engineers compete for limited resources, particularly for something that is not a functioning part of the system such as systems engineering documentation that may not be required for years? This is unlikely to receive serious attention from the PM given all of the things to be dealt with in the PM's politically charged world unless the engineers can communicate their needs in a way that gains clarity through the PM's lens.

To understand the organizational cognitive lenses or paradigms better, (Bolman and Deal, 1997) explore the concept of framing by stating, "A frame is a coherent set of ideas that enable you to see and understand more clearly what goes on day to day" (p. 41). A frame is a set of ideas or assumptions that help you understand and negotiate a particular "territory." Like maps, frames are both windows on a territory and tools for navigation.

The Bolman and Deal (1997) Four-Frame Model (Table 4) proposes four lenses in which leaders can view the world. For this research, the focus will be on the Political Frame, the frame from which the PM operates, and the Structural Frame, the frame from which the SE operates.

	Frame			
	Structural	**Human Resource**	**Political**	**Symbolic**
Metaphor for organization	Factory or machine	Family	Jungle	Carnival, temple, theatre
Central concepts	Rules, roles, goals, policies, technology, environment	Needs, skills, relationships	Power, conflict, competition, organizational politics	Culture, meaning, metaphor, ritual, ceremony, stories, heroes
Image of leadership	Social architecture	Empowerment	Advocacy	Inspiration
Basic leadership challenge	Attune structure to task, technology, environment	Align organizational and human needs	Develop agenda and power base	Create faith, beauty, meaning

Table 4. Four Frame Model (From: Bohlman and Deal, 1997)

To make sense of the political environment in which the PM operates, the Political Frame is the cognitive model applied. Five propositions summarize this perspective (Simon, 2007).

- Organizations are coalitions of various individuals and interest groups
- There are enduring differences among coalition members in values, beliefs, information, interest, and perceptions of reality
- Most important decisions involve the allocation of scarce resources-who gets what
- Scarce resources and enduring differences give conflict a central role in organizational dynamics and make power the most important resource
- Goals and decisions emerge from bargaining, negotiation, and jockeying for position among different stakeholders

Particularly in the project planning phase, the bargaining, negotiation, and jockeying in proposition 5 are at a peak. The PM's decision to resource systems engineering documentation is weighed against all of the other competing efforts, and more often than not, is determined not to be critical, or even competitive. The comprehensive risk model proposed in Chapter V presents the requirement for resourcing in the PM's cognitive frame, in terms of risk. The work can then be resourced to the desired risk level, with the PM accepting the residual risk.

From personal experience, the inability of the Navy Working Capital Fund organizations, i.e., the Warfare Centers, to communicate with the PM in their frame, results in critical technical work not being resourced. The Structural Frame is the cognitive frame, from which the SE operates. Six assumptions undergird the Structural Frame (Simon, 2007):

- Organizations exist to achieve established goals and objectives
- Organizations work best when rationality prevails over personal preferences and external pressures
- Structures must be designed to fit an organization's circumstances (including its goals, technology, and environment)
- Organizations increase efficiency and enhance performance through specialization and division of labor
- Appropriate forms of coordination and control are essential to ensuring that individuals and units work together in the service of organizational goals
- Problems and performance gaps arise from structural deficiencies and can be remediated through restructuring

The Structural Frame is markedly different from the Political Frame. Rational thought prevails, not competition and negotiation. In the context of critical systems engineering documentation, two prevailing problems must be overcome. First, the systems engineering leadership would provide a cost and schedule estimate for the technical work based on input from Subject Matter Experts (SME). This estimate would compete for resources with other program efforts. The systems engineers would not view this as work that should be competed for, but simply, as work that must be done.

The likelihood that the estimate would compete well is small, and in fact, experience has shown this to be true. Table 5 provides the status of required ISPs for the Marine Air/Ground Task Force Command and Control, Weapons, and Sensors Development and Integration (MC2I) Product Group (PG) at Marine Corps Systems Command (MCSC) and shows that 92.3% (12 of 13) active efforts are late.

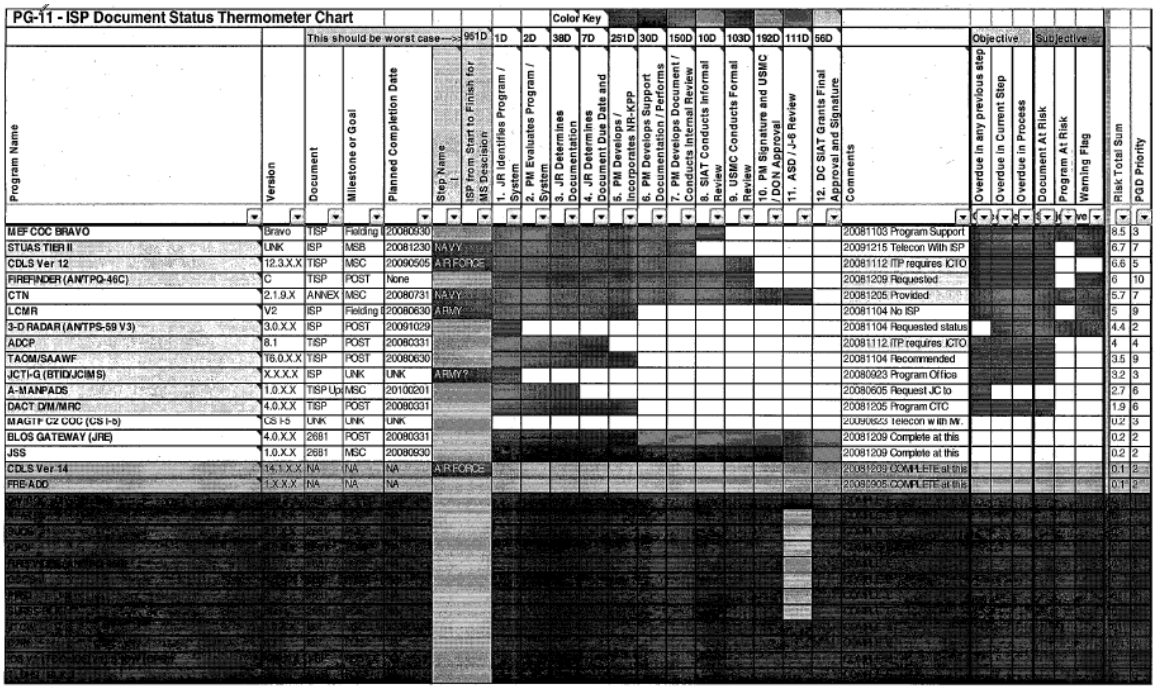

Table 5. MCSC MC2I PG ISP Status December 18, 2008

A questionnaire (Table 6) was provided to the Architecture Center of Excellence (COE) at SPAWAR–Atlantic (SSC-L) to gain insight into the reasons for the above ISP status.

Question	Response
1. For each node in the ISP development network previously provided, what are the costs for each node, both labor and resources, in units relative to node times ($/day)?	SPAWAR does not have the data to provide sufficient details there. They recommend strongly that no costs be assigned to the nodes shown in the ISP development network diagram. It is well documented that ISPs, beginning to final acceptance, can vary in costs anywhere from $150K to $3M depending on project scope and solution provided. Additionally, labor and resources are both

Question	Response
	directly impacted by project complexity and size, making it impossible to assign values to the nodes without applying the process to a specific program.
2. What is the cause of the variance at each node? a. Rework b. Difficulty of task c. Availability of resources d. Knowledge of subject/task not adequate e. Technical work uncovers errors or inconsistencies in previous tasks/nodes that must be adjudicated f. Inadequate tools g. Incomplete planning for tasks for that node h. Other (please specify/describe)	a. Rework does not apply to development node variance within this process. Nodes 19, 21 and 23 capture rework times. b. Difficulty of task is the major cause of variance of all nodes. c. Availability of resources should be scoped at start, and therefore, minimized at each node. d. Inadequate knowledge of subject/task is the second major variance of all nodes. e. Not a major consideration on node variance due to the nature of node start times being directly dependant on the completion of previous nodes. f. Required tools should be scoped at start, and therefore, minimized variance at each node. g. If the process is followed, planning is largely taken care of by process flow. No major cause of variance. h. Other (please specify/describe)
3. Are labor and resource requirements identified to the PM prior to commencing ISP development per the network diagram provided?	History has shown that the PM do not typically plan for ISP/Architecture development early enough in the acquisition process, largely due to a lack of understanding of what the documents are and what their intended uses are.
4. In your opinion, does the PM understand the effort (time, resources, and process) required to develop and gain ISP approval prior to commencement of ISP development?	No. Training must be provided to each PM to lay out in simple terms the ISP development process and what resources are required to complete it. These resources do not only include architects and tools, but critical program documentation and SMEs who must be integrated into the process from the beginning. Furthermore, it is unrealistic for PMs to be expected to stay current on ISP/Architecture standards, development and policy changes. Continuous expertise must be maintained in this area and relayed accordingly back to the PMs. NOTE: All PMs are trained that an initial ISP is developed to support the ICD, then further developed for the CDD, and further elaborated for the CPD or during production. The reality is that the absence of JCIDS documents means ISPs are developed during or post milestone C, which means the prep-work normally done is all rolled up into a single document and bolted onto a product.
5. Provide any other thoughts or information that need to be quantified to plan this work better.	PMs must be educated that ISPs/Architectures are the front end of engineering, not bolt-on products after the fact. Recommend adopting strategic goals and objectives to include measures associated with IA, ISPs and IATOs at the PM and MSIT level. This is a culture change that must take place to achieve

Question	Response
	quality systems acquisition with shrinking budgets. ISPs/Architectures can be expensive to create, but their use and reuse provides significant ROI across the PG.
6. Identify the node or nodes and the reason for the red status (should be from 2. above) provided in the 12/18/08 ISP status table.	Without clarification from the creator of the 12/18/08 ISP status table as to how the color designations were assigned, no correlation between the status table and the ISP development process can accurately be made. Basically, the sheet was created for Mike Ferraro by Tim King without any documented logic but as a way to track the ISP administratively in MCSC staffing process.

Table 6. SSC-L Architecture COE Questionnaire (From: SSC-L Architecture COE, June 2009)

The response to question 2b regarding variance, indicates a strong presence of uncertainty in the technical work itself. Responses to questions 4 and 5 point directly to the framing problem previously discussed, particularly during project planning.

The second problem to overcome is that the technical work and assembly of the document is estimated and then performed by the systems engineering organization. Their estimate and goal (success) is to complete that document. The subsequent review and certification process is in the hands of the PM's organization and is performed very much in a political environment where negotiation and advocacy are the norm. Essentially, this document is subject to a difficult frame transition without an end-to-end estimate of resources. The comprehensive risk model proposed in Chapter V accounts for all three of these challenges.

D. SUMMARY

This chapter explored the influences of individual and organizational behaviors, and the environment in which these organizations operate, on the ability of the project team to solve problems and be successful. An effective risk management plan must be implemented at the worker level and be an integral part of project planning and

execution. For that to occur, a thorough understanding on how the diverse organizations that comprise a project team see the world is required. Only when individual workers are effective and resourced can the project be successful.

A common understanding between the systems engineering and project management organizations on program success can be found by beginning with the end in mind (Covey, 1998). Through proactive leadership, the team can get their arms around both the things they can control and better understand those they cannot to define the steps needed for success. Those uncertainties inherent in things outside of the project team's influence can be addressed through effective risk management.

Framing theory (Bohlman & Deal, 1997) provides insight into how the different environments the PM and SE operate in affect the decision making process. The political world of the PM, dominated by constrained resources, negotiation, and agendas is far different from the rational in which world engineers operate. Bridging this gap is critical to the success of the project, particularly in the planning phase when scarce resources are negotiated for and allocated.

Lastly, the data collected from the SSC-L Architecture COE (June 2009) points directly to these behavioral and environmental influences as a major cause for the 92.3% late status. The PM simply does not resource this work up front, but apply pressure and resources too late. The technical difficulty of the task is the main contributor to the variance. This uncertainty can be addressed through the implementation of effective risk management practices. However, with the responsibility for the successful approval of the ISP dependent on the effectiveness of both the PM and engineering organizations, the risk approach for the ISP must be an end-to-end approach to address uncertainties in both environments.

Chapter V proposes a comprehensive risk model that considers the end-to-end challenges, explored in the first four chapters, of developing and approving complex systems engineering documentation required by both statute and regulation for program success.

THIS PAGE INTENTIONALLY LEFT BLANK

V. ISP QUANTITATIVE RISK MODEL

A. INTRODUCTION

Systems engineering documents, as required by statute and regulation for DoD weapon, and IT systems acquisition, are as important to program success as the effectiveness, suitability, and affordability of the system itself. The ISP, being one of the most complex systems engineering documents, has been the focus of this research. Chapters I through IV explored the JCIDS and DoD acquisition framework requirements for the ISP, the need to address the risks early in the planning phase, the human and environmental influences on risk management, and examined data from the Architecture COE.

This chapter proposes a risk model for the development of the ISP that begins with the end in mind, approval of the ISP. By representing the end-to-end process as a comprehensive single network, two previously explored critical points of failure are addressed. First, the efforts for both the systems engineering and PM organizations are represented in the network so that the entire effort can be planned, proactively and with the end in mind. The activities, expressed as nodes in the network, were provided by the Architecture COE. Program Evaluation and Review Technique (PERT) was used for scheduling of the network. Critical Path analysis was then performed and a cumulative probability distribution function calculated.

Second, by providing a quantitative risk assessment for the comprehensive network, the frame transition issues between the SE and PM are overcome through common risk based communications. In other words, the PM accepts the risks associated with the level of resources the PM provides, per a cumulative probability distribution function.

B. ISP NETWORK DIAGRAM

The ISP, as previously discussed, is a systems engineering document that is the technical artifact capturing the results of extensive and complex technical work. Without this technical effort, battlefield interoperability is unlikely to be realized and I&S certification not achieved. Figure 10 provides the scheduling of all the technical work, document assembly, and multi-organizational reviews for completion and approval of the ISP. Note that there is a sequence for development of the DODAF views that must be followed, which creates dependencies captured in the network diagram.

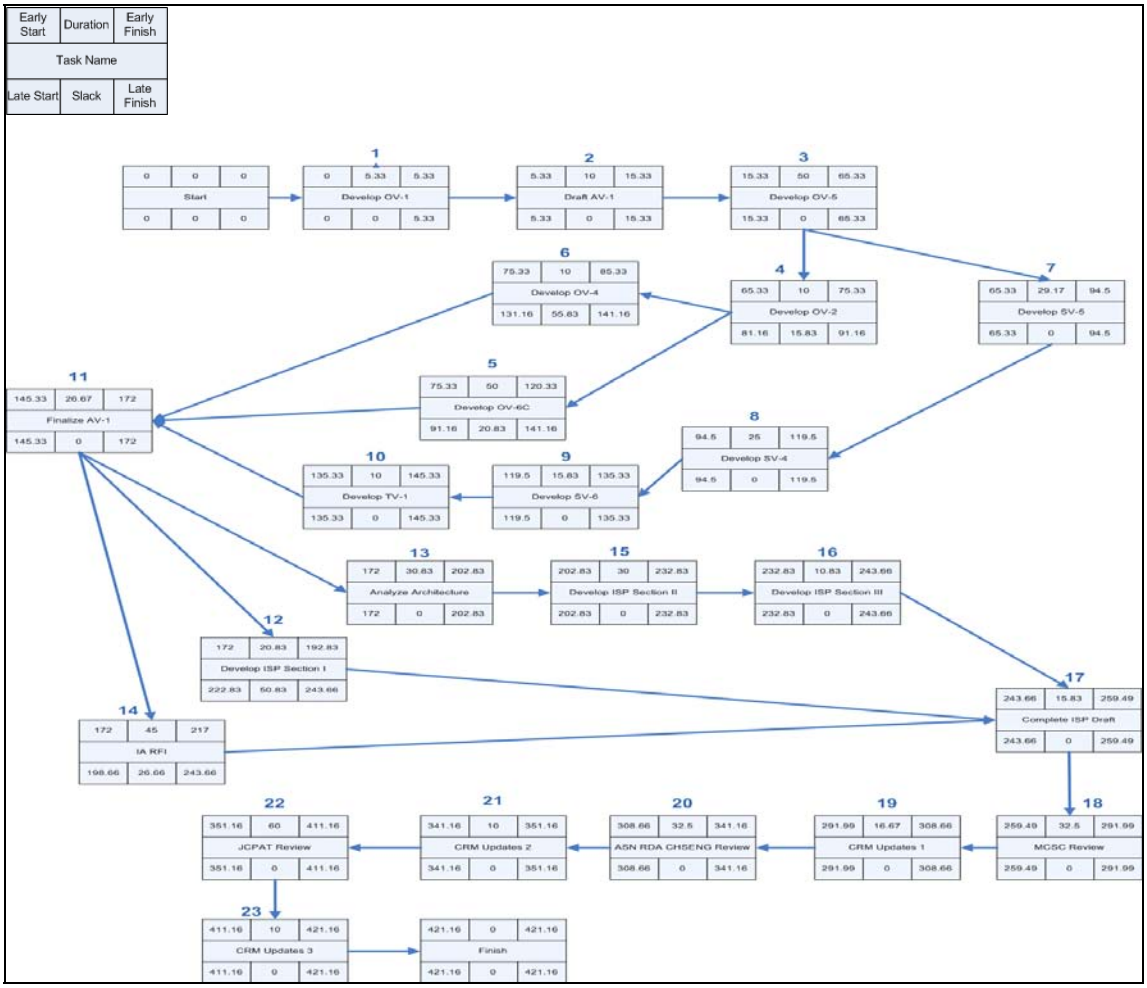

Figure 10. ISP Development Network (From: SSC-L Architecture COE, June 2009)

In addition to the sequential nature of the work, the DODAF views are generated by multiple organizations with the Operational Views (OV) being the responsibility of the requirements organizations, and the System Views (SV) the responsibility of the engineering arm of the acquisition organization. There is also an iterative aspect to the DODAF view development. Node 11 finalizes the All View (AV)-1 developed as a draft in Node 2. Also, Node 13 is where the architecture analysis occurs and resultant changes implemented into the DODAF views as needed. The start, stop, and duration times for each node were generating using the PERT approach explored in the next section.

The three main efforts required for ISP approval are all represented in the comprehensive network. These efforts include the following:

1. The generation of the DODAF views, Nodes 1 through 11 and 13
2. The assembly of the ISP document, Nodes 12 through 17
3. The multi-organizational review and approval, Nodes 18 through 23

The frame transition issues discussed in Chapter IV can be seen in the network and occur at Node 1 where the PM has not resourced the work up front (Architecture COE, June 2009), and at Node 18 when the PM's organization has to push the document through the local, Service, and Joint review process, each with a unique perspective.

With the comprehensive project network in place, the next steps are to estimate the efforts, determine the critical path, and perform quantitative risk assessment.

C. PERT ANALYSIS

With the previously discussed complexities of ISP development and approval, captured in the single comprehensive project network, the PERT approach was applied for project scheduling. Nahmias (2005) recommends PERT when uncertainty in activity times is present because PERT estimates provide the effects of uncertainty on the project completion time. In addition to the uncertainty perspective, PERT was chosen because of the non-threatening approach to estimating. Had Critical Path Method (CPM) been used, the minimum completion times for each node would have to be estimated by the SE and PM. Given both that this is the initial attempt to capture the end-to-end process in a single project network, and the lack of historical data (SSC-L Architecture COE, June 2009),

the SE and PM were not comfortable with providing a deterministic estimate. This is important since an effective risk management plan is implemented at the worker level. To gain worker buy-in and trust for this new process, allowing uncertainties in their ability to estimate is key to effective implementation.

The PERT approach has the SMEs provide three estimates; best or optimistic (a), worst or pessimistic (b), and most likely (m). These estimates are then used to construct a beta distribution for each node of the network. By assuming the activity times are independent random variables, a mean, standard deviation, and variance can be calculated for each node using the following formulas (Nahmis, 2005, p. 508).

- Mean $(\mu) = (a + 4m + b)/6$
- Standard Deviation $(\sigma) = (b - a)/6$
- Variance $(\sigma^2) = (b - a)^2/36$

The central limit theorem is then used to justify a normal distribution.

> The central limit theorem says that the distribution of the sum of independent random variables is approximately normal as the number of terms is the sum grows large. Convergence occurs rather quickly. (Nahmis, 2005, p. 509)

The PERT approach then assumes that the critical path is the path with the longest expected completion times (μ). The next section explores the critical path analysis and results. The total project time is a sum of critical activities and is assumed to be normally distributed, as previously discussed.

The PERT estimates given in Table 7 were provided by the Architecture COE with the mean/expected times (μ) and variance (σ^2) calculated as per the equations provided above.

Node	Activity	Optimistic (a)	Most Likely (m)	Pessimistic (b)	Expected (μ)	std dev (σ)	variance (σ^2)
1	Develop OV-1	2	5	10	5.33	1.33	1.78
2	Draft AV-1	5	10	15	10.00	1.67	2.78
3	Develop OV-5	30	45	90	50.00	10.00	100.00
4	Develop OV-2	5	10	15	10.00	1.67	2.78
5	Develop OV-6C	30	45	90	50.00	10.00	100.00
6	OV-4	5	10	15	10.00	1.67	2.78
7	SV-5	15	25	60	29.17	7.50	56.25
8	SV-4	10	20	60	25.00	8.33	69.44
9	SV-6	5	15	30	15.83	4.17	17.36
10	TV-1	5	10	15	10.00	1.67	2.78
11	AV-1	15	25	45	26.67	5.00	25.00
12	Develop ISP Sec I	15	20	30	20.83	2.50	6.25
13	Analyze Arch	20	30	45	30.83	4.17	17.36
14	IA RFI	30	45	60	45.00	5.00	25.00
15	Develop ISP Sec II	15	30	45	30.00	5.00	25.00
16	Develop ISP Sec III	5	10	20	10.83	2.50	6.25
17	Complete ISP Draft	10	15	25	15.83	2.50	6.25
18	MCSC ISP Review	15	30	60	32.50	7.50	56.25
19	CRM Updates 1	10	15	30	16.67	3.33	11.11
20	Asn RDA Review	15	30	60	32.50	7.50	56.25
21	CRM Updates 2	5	10	15	10.00	1.67	2.78
22	JCPAT Review	30	60	90	60.00	10.00	100.00
23	CRM Updates 3	5	10	15	10.00	1.67	2.78
	Total Days	**302**	**525**	**940**	**557**		

Table 7. PERT Estimates for ISP Network (From: SSC-L Architecture COE, June 2009)

A quick analysis of the node results shows significant variance of more than 50 days for 30%, or seven of the 23 nodes. The effects of this can be seen back in the total optimistic and pessimistic difference of 638 days. To put this difference into perspective, a PM plan based on optimistic ISP development time, could be under estimated by almost a year and nine months. Recalling that the ISP is a required document for milestones and fielding, significant schedule risk is obvious and requires a proactive and effective risk management effort. With the activity times estimated, the PERT process continues in the next section with an exploration of the critical path for the ISP network. Once the critical path is determined, project schedule and probability of success can be calculated.

D. CRITICAL PATH ANALYSIS

The critical path for a project network is defined as the longest path (in time) through the network since this is the minimum time in which the project can be completed. Nahmias' (2005) process for determining the critical path was applied to the

ISP network. A forward pass through the network using the mean duration, or expected times, for each activity was performed to find the early start and finish times. A backward pass was then made to find the latest start and finish times. Table 8 provides the results.

Activity	Mean Duration(μ)	Early Start (ES)	Early Finish (EF)	Late Start (LS)	Late Finish (LF)	Slack LS-ES	Slack LF-EF	Critical Path =1
1	5.33	0.00	5.33	0.00	5.33	0.00	0.00	1
2	10.00	5.33	15.33	5.33	15.33	0.00	0.00	1
3	50.00	15.33	65.33	15.33	65.33	0.00	0.00	1
4	10.00	65.33	75.33	81.16	91.16	15.83	15.83	0
5	50.00	75.33	125.33	91.16	141.16	15.83	15.83	0
6	10.00	75.33	85.33	131.16	141.16	55.83	55.83	0
7	29.17	65.33	94.50	65.33	94.50	0.00	0.00	1
8	25.00	94.50	119.50	94.50	119.50	0.00	0.00	1
9	15.83	119.50	135.33	119.50	135.33	0.00	0.00	1
10	10.00	135.33	145.33	135.33	145.33	0.00	0.00	1
11	26.67	145.33	172.00	145.33	172.00	0.00	0.00	1
12	20.83	172.00	192.83	218.66	239.49	46.66	46.66	0
13	30.83	172.00	202.83	172.00	202.83	0.00	0.00	1
14	45.00	172.00	217.00	194.49	239.49	22.49	22.49	0
15	30.00	202.83	232.83	202.83	232.83	0.00	0.00	1
16	10.83	232.83	243.66	232.83	243.66	0.00	0.00	1
17	15.83	243.66	259.49	243.66	259.49	0.00	0.00	1
18	32.50	259.49	291.99	259.49	291.99	0.00	0.00	1
19	16.67	291.99	308.66	291.99	308.66	0.00	0.00	1
20	32.50	308.66	341.16	308.66	341.16	0.00	0.00	1
21	10.00	341.16	351.16	341.16	351.16	0.00	0.00	1
22	60.00	351.16	411.16	351.16	411.16	0.00	0.00	1
23	10.00	411.16	421.16	411.16	421.16	0.00	0.00	1
TOTAL PROJECT TIME =	421.17	days						
Project Std Deviation (σ) =	85.50	days						

Table 8. ISP Network Critical Path Analysis Results

By identifying the activities that have no slack time, the critical path can be found since any delay in those tasks delays the start of the next task, thus causing a delay in the project completion. The critical path is indicated in red in Table 7. An Excel spreadsheet model was created to identify the critical path (last column) by returning a "1" and the slack times were "0."

The critical path for the ISP network is activities; 1-2-3-7-8-9-10-11-13-15-16-17-18-19-20-21-22-23, or 18 of the 23 nodes (78.3%). Any slip in one of those nodes causes a delay in the ISP approval. With only one node (Node 5) with a variance greater than 50 days that is not on the critical path, this is another indicator that the ISP development and approval is a very risky project.

The total project time of 421.17 days is found by summing the mean duration (μ) times for the critical path. The project standard deviation (σ) of 85.50 days is found by summing the standard deviations of the nodes on the critical path.

The 421 days the project is mostly to take to complete is 119 days more than the optimistic estimate of 302 days. By using the PERT approach, which accounts for the uncertainty in each of the nodes, a more accurate estimate based on the most likely times has been found. With more than 78% of the nodes on the critical path, and with six of the seven nodes having a variance of greater than 50 days also on the critical path, the ISP development and approval project has a significant amount of risk exposure that must be managed. The estimate for both the project duration and project standard deviation can now be used for quantitative risk assessment.

E. ISP CUMULATIVE PROBABILITY DISTRIBUTION FUNCTION

The project duration and standard deviation calculated using the PERT approach in the previous section can now be used to perform a quantitative risk assessment of the comprehensive ISP network. As discussed previously, the central limit theorem justifies the use of a normal distribution. Table 9 contains the results of the NORMINV Excel function for probabilities between 0 and 1. The NORMINV function returns the inverse of the normal cumulative distribution function for a given mean and standard deviation and is used to find the cumulative probability distribution function. The NORMINV function is used since the probability of success is the probability that the risk does not occur, or the inverse of the normal distribution for the probability of occurrence.

Probability	Days	Probability	Days
0.01	222.26	0.55	431.91
0.05	280.53	0.6	442.83
0.1	311.59	0.65	454.11
0.15	332.55	0.7	466.00
0.2	349.21	0.75	478.84
0.25	363.50	0.8	493.13
0.3	376.33	0.85	509.78
0.35	388.22	0.9	530.74
0.4	399.51	0.95	561.80
0.45	410.42	0.99	620.07
0.5	421.17		

Table 9. ISP Network Probability

The results show that if the project is resourced for 421 days, only a 50% probability exists that the project is complete. Since 421 days was the expected time, or mean (μ), that does make sense. Given the uncertainty in the independent random variable that each node represents, the data also shows that if 99% chance of success is desired by the PM, the project would need to be resourced for 620 days, which is actually 199 days longer than the expected project time (μ).

Figure 11 provides a graphical plot of the cumulative distribution.

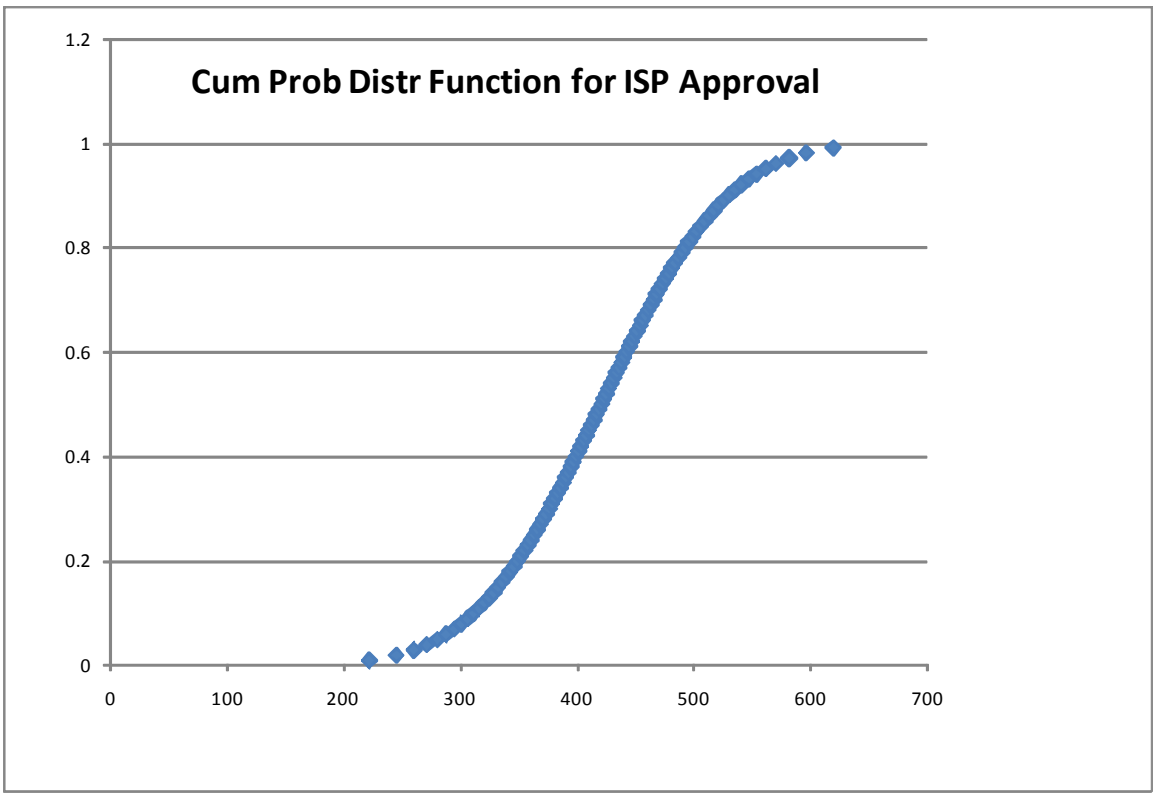

Figure 11. ISP Network Cumulative Probability Distribution Function

From the plot, it is easy to visualize the first 400 days of project time only yields a probability of success of 40 percent. An investment of an additional 93 days increases the probability of success to 80%, which is a typically acceptable risk in project management. The intent is that through visualization, the PM, MDA, and stakeholders can quickly understand the risk associated with a given level of resourcing for systems engineering documentation. From that understanding, either the risk can be accepted or additional action taken until the risk is of an acceptable level.

F. SUMMARY

"A risk may or may not happen, and you will not know for sure until the risk occurs, that is–until after it ceases to be a risk. This inherent uncertainty cannot be eliminated. However, you can often narrow the uncertainty by clarifying the probability of occurrence of the risk" (Smith and Merritt, 2002, p. 5). This chapter explored the

application of the PERT approach to quantify the risks associated with the ISP development and approval process. PERT was selected as the network scheduling approach because of the uncertainty associated with each of the activities (nodes) in the comprehensive project network.

The project network and node estimates were provided by the SSC-L Architecture COE (June 2009). The project network is an end-to-end, or comprehensive network, that considers the DODAF, document assembly, and organizational, Service, and Joint review processes so that the risk can be quantified for the entire project, begun with the end in mind.

The most likely project time, calculated using the PERT approach, was 421 days, with 18 of the 23 nodes (78.3%) on the critical path. The 421 days most likely, or mean (μ) project time, is 119 days longer than the 302 day optimistic effort provided by the SSC-L Architecture COE. This implies that a PM who resourced the optimistic effort was likely to underestimate the project by four months, putting milestones and other decision points at significant risk.

In fact, the cumulative probability distribution function results show that there is only a less than 10% probability of success for the optimistic effort, and a 50% chance of success for the most likely estimate. For the project to have an 80% chance of success, the ISP network must be resourced for 493 days, or 191 days more than the optimistic estimates or 72 days more than the most likely.

The overarching intent of implementing a quantitative risk assessment approach for the ISP that looks at the cumulative probability distribution function is to provide a clear understanding, through visualization of the risks associated with the resourcing level of a critical systems engineering document, required by both statute and regulation. PMs, MDAs, and stakeholders can then either accept the risk, or take action to reduce it.

With the risk model generated, answers to the questions posed in Chapter I can now be provided. Chapter VI summarizes the research and findings of this thesis, answers the research questions, identifies lessons learned, and provides recommendations for further research.

VI. CONCLUSION

A. SUMMARY OF KEY RESEARCH FINDINGS

Chapters I through V explored the need for risk management, the human element in decision making, and the quantification of risk. This chapter provides the answers to the research questions outlined in Chapter I, lessons learned, and recommendations for further research.

The research has shown that systems engineering documentation, required by statute and regulation for DoD acquisition of Weapon, NSS, and IT systems, are technical artifacts resulting from significant technical effort and subjected to complex review and approval processes. The uncertainties in both efforts expose the document, and subsequently the program, to risks that must be effectively managed. The ISP, due to the significance of the document to the acquisition process and its inherent complexity, was the focus of the research.

Data from the SSC-L Architecture COE (2009) showed that the effort for the ISP is neither properly resourced nor understood by the PM and that the document's development is not managed as part of the acquisition program, but rather as a "bolt-on." As of December 2008, greater than 92% of the ISPs under development for MCSC by the Architecture COE were late.

At the request of the author, an end-to-end ISP project network was developed by the Architecture COE. From this network, the PERT approach was applied and a quantitative risk assessment model developed to generate a cumulative probability distribution function. This quantitative risk assessment approach was chosen to both overcome the environmental and human behavioral differences inherent in the PM and engineering organizations that impede communications as well as to provide a clear, quantified indication of risk that can either be acted upon by the PM or accepted.

B. ANSWERS TO RESEARCH QUESTIONS AND LESSONS LEARNED

1. Can the Risk to a Required DoD Systems Engineering Artifacts be Quantified?

An end-to-end project network for the ISP, a key systems engineering document required by statute and regulation, was developed and a quantitative risk assessment performed on that comprehensive project effort. It is important to note that the methodology proposed in this research delivers a single quantifiable risk assessment for the entire ISP, inclusive of the DODAF technical work, document assembly, and local, Service, and Joint review and approval processes. By generating this single probability of success for the ISP, the risks can either be accepted or acted upon by the PM early in the project, during project planning activities.

This single probability of success provides common ground for the PM and SE to communicate thereby bridging the frame transition issues created by differing perspectives researched in Chapter IV. The communication issue was verified by data provided by the Architecture COE and resulted in under resourced ISP efforts and subsequently a 92.3% late or at risk status for MCSC ISPs under development by the Architecture COE.

The PERT approach for project scheduling was used for this research due to the uncertainty in the ISP development and approval process and the lack of historical data. Three estimates (best, worst, and most likely) for each activity or node were developed under PERT allowing the systems engineers to not feel threatened by having to provide a single deterministic estimate. This sensitivity to the SE's perspective facilitates worker buy in, and subsequently, implementation of risk management at the lowest levels of the organization. As explored in Chapter III, implementation at the worker level is required for effective risk management.

The cumulative probability density function, calculated from the project estimating, scheduling, and critical path identification PERT results, provides a clear visualization for the PM, MDAs, and stakeholders to see the probability of success (approval of the ISP) expected from the resourcing level provided by the PM. The

research in Chapter V shows that an 80% probability of success requires the PM to resource the ISP project 493 days, 119 days longer than the optimistic estimate of 302 days. Additionally, the ISP project is extremely sensitive to the resourcing level. Should a PM resource the project for 400 days, less than a 19% reduction in estimated resources, probability of success drops to 40 percent.

In closing, the research clearly shows that the risks can be quantified for one of the most complex systems engineering documents in DoD acquisition. The methodology, due to the end-to-end approach, also facilitates the implementation of an effective risk management approach for systems engineering documentation.

2. Does the Quantification of Risk Support the Transition from the Rational to the Political Frame during Project Planning?

Chapter IV research reveals that the PM and SE have different perspectives created by the environments in which they must operate. These frames, or lenses through which the world is viewed, affects decision making and ultimately problem solving. With the uncertainty and complexity resident in the ISP project, each organization has problems that must be solved. The SE have to complete difficult technical work in the generation of DODAF architectures or battlefield interoperability is not achieved. The PM must make difficult resourcing decisions in a resource-constrained environment to fund the technical work and must shepherd the document through the local, Service, and Joint review processes.

The methodology proposed in this research delivers a quantitative risk assessment for the end-to-end ISP development, review, and approval process. It begins with the end in mind. The probability of success is calculated from the comprehensive (DODAF architecture development, document assembly, review and approval) project network resulting in a single statistically based assessment of risk that provides the common ground for PM and SE to communicate. Early in the project, during project planning when resourcing decisions are made, the PM can accept the risks associated with resourcing decisions and given those decisions, expectations are clear for the SE.

3. What Changes to the CMMI Project Planning Process Area should be Considered?

The Project Planning (PP) process area has three Specific Goals (SG) and Specific Practices (SP) associated with each SG. As explored in Chapter IV, PP is where the project team gets their arms around the uncertainties and realities associated with the project, by establishing estimates (SG 1), developing a project plan (SG 2), and obtaining commitment to the plan (SG 3). Based on the research, the following changes are recommended for the PP process area:

Specific Practice (SP)	Title	Recommended Change
SP 1.1	Estimate the Scope of the Project	Modify sub-practice 1; **Develop a WBS based on the product architecture.** Add: - Tasks for development of critical systems engineering documents or artifacts, such as SEP and ISP.
SP 1.2	Establish Estimates of Work Product and Task Attributes	Add new sub-practice: **3. Estimate Effort for critical systems engineering documents, i.e., SEP and ISP.** Estimate scope to include technical effort, document assembly, review and approval process, and comment adjudication.
SP 1.4	Determine Estimates of Effort and Cost	Add new sub-practice: **4. Include critical systems engineering documents when estimating effort and cost.** Modify sub-practice 3; Estimate effort and cost using models and/or historical data: Add: - Required systems engineering documents or artifacts - Review and approval process for systems engineering documents and artifacts
SP 2.1	Establish the Budget and Schedule	Modify 4. Identify task dependencies: Add: Include required systems engineering documents and artifacts when scheduling project tasks.
SP 2.2	Identify Project Risks	Modify 1. Identify risks: Add: Risks must be identified for the development, review, and approval of required systems engineering documents.

Table 10. Changes to the CMMI Project Planning Process Area

4. What Changes to the CMMI Risk Management Area Should be Considered?

The Risk Management (RSKM) process area has three Specific Goals (SG) and Specific Practices (SP) associated with each SG. The CMMI (2007) risk management approach is consistent with the research, promoting early identification of the risks during project planning. Prepare for Risk Management (SG 1), Identify and Analyze Risks (SG 2), and Mitigate Risks (SG 3) are the specific goals to achieve in this process area. Based on the research, the following changes are recommended for the PP process area:

Specific Practice (SP)	Title	Recommended Change
SP 1.1	Determine Risk Sources	Add: - Uncertainty in technical work for required systems engineering documents and artifacts - Uncertainty in systems engineering review and approval processes.
SP 1.3	Establish a Risk Management Strategy	Modify paragraph 1: Change bullet 1 to read: The scope of the risk management effort to include required systems engineering documents and artifacts. Change bullet 3 to read: Project-specific sources of risks to include internal and external systems engineering documents/artifacts review and approval processes.
SP 2.1	Identify Risks	Modify sub-practice 1. Sentence to read: Schedule risks may include risks associated with planned activities, key events, and milestones to include required systems engineering documents/artifacts Add new sub-process: **Quantify risks for required systems engineering documents and artifacts.** Perform quantitative a risk assessment by generating a cumulative probability distribution function for the end-to-end systems engineering document effort inclusive of technical work, document assembly, and the review and approval process.

Specific Practice (SP)	Title	Recommended Change
SP 2.2	Evaluate, Categorize, and Prioritize Risks	Add new sub-practice: **Evaluate probability of success for systems engineering documents and artifacts.** Evaluate the probability of success expected from the planned resourcing level and either accept the risk or take action on resourcing levels.

Table 11. Changes to the CMMI Risk Management Area

5. Does Inclusion of Risk Quantification into Key Systems Engineering Documents during Project Planning Improve the Probability of DoD Program Success?

The research has established the relationship, by statute and regulation, of systems engineering documents to progression through the DoD acquisition framework. Directly, DoD weapons, and IT systems cannot progress through development and fielding without approval of required systems engineering documents thereby preventing capability from being delivered to the warfighter. Without capability delivery, the project cannot be successful.

Although the improvement to the probability of program success was not calculated, the research shows that through the creation of an end-to-end project network, and calculation of a cumulative distribution function for quantitative risk assessment, for the first time, the risks inherent in these complex documents can be addressed early in project planning. With the risks understood by all, the entire project, to include required systems engineering documents, can now be planned and managed through milestone decisions and fielding to the warfighter thereby improving the chance of success: maintaining U.S. advantage on the battlefield.

C. FUTURE RESEARCH

The following topics related to risk management should be considered for future research:

- Generate comprehensive project networks for JCIDS capabilities documents and conduct a quantitative risk assessment. Although not the PM's responsibility, these documents are very similar in both technical and review/approval process complexity. These documents are also required by statute and regulation.
- Investigate implementation of this quantitative risk model into the Department of the Navy Probability of Program Success (POPs) approach for program health assessment
- Investigate implementation of this quantitative risk model into the Department of the Defense Risk Management Guide for DoD Acquisition (August 2006)

The complexities of developing and acquiring the weapon and IT systems needed for an advantage on today's battlefield requires that all contributing organizations work toward a common goal. It is a human endeavor. Finding common ground that accepts the diverse environments in which decisions are made is critical for the DoD acquisition community to deliver for those who defend us. Continued research in this area, to tie process and decision making together, can foster the behaviors' needed for success.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Agnes, M. (Ed.). (2006). *Webster's new world college dictionary* (4th ed.). Cleveland, OH: Wiley.

Ayyub, B. (2003). *Risk analysis in engineering and economics*. Boca Raton, FL: Chapman & Hall/CRC.

Blanchard, B., & Fabrycky, W. (2006). *Systems engineering and analysis* (4th ed.). Upper Saddle River, NJ: Pearson Prentice Hall.

Bolman, L., & Deal, T. (1997). *Reframing organizations* (2nd ed.). San Francisco, CA: Jossey-Bass.

Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6212.01E. (2008, December 15). *Interoperability and supportability of information technology and national security systems*.

Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3170.01G. (2009, March 1). *Joint capabilities integration and development system*.

Chrissis, M. B., Konrad, M., & Shrum, S. (2007). *CMMI guidelines for process integration and product improvement* (2nd ed.). Boston, MA: Pearson Education, Inc.

Clemen, R., & Reilly, T. (2001). *Making hard decisions with decision tools*. Pacific Grove, CA: Brooks/Cole.

Conrow, E. H. (2003). *Effective risk management: Some keys to success*. Reston, VA, AIAA.

Covey, S. (1989). *The 7 habits of highly effective people*. Provo, UT: Covey Leadership Center.

Department of Defense Guide. (2006, August). *Risk management guide for DoD acquisition*.

Department of Defense Instruction 5000.2. (2008, December 8).*Operation of the defense acquisition system*.

Forsberg, K., PhD, Mooz, H., & Cotterman H. (2000). *Visualizing project management: models and frameworks for mastering complex systems* (2nd ed.). New York: John Wiley & Sons.

Gruhl, W. (2004). *Value of systems engineering; Summary report*. NASA Comptroller's Office.

Haimes, Y. Y. (2004). *Risk modeling, assessment, and management*. Hoboken, NJ: Wiley-Interscience.

MARCORSYSCOM Order 5000.3. (2008, June 6). *Naval SYSCOM risk management policy*.

Marine Corps Systems Command. MC2I Product Group. (2008, December). Quantico, VA.

Nahmias, S. (2005). *Production & operations analysis* (5th ed.). New York, NY: McGraw-Hill.

Office of the Assistant Secretary of the Navy Research. Development, and Acquisition Memorandum for Distribution. (2008, October 6). *Implementation guidance and methodology for Naval Probability of Program Success (PoPS).*

Ragsdale, C. (2007). *Modeling and spreadsheet analysis* (5th ed.). Mason, OH: Thomson South-Western.

Simon, C. (2007). *Notes for MN 3117 (Organizational processes*). Naval Postgraduate School, Monterey, CA. (Unpublished).

Smith P. G. & Smith G. M. (2002). *Proactive risk management: Controlling uncertainty in product development*. New York, NY: Productivity Press.

SPAWAR Systems Center-LANT Architecture Center of Excellence. (2009, June). Charleston, SC.

Ulrich, K. T., & Eppinger, S. D. (2008). *Product design and development* (4th ed.). New York, NY: McGraw-Hill.

Wagner III, J., & Hollenbeck, J. (1992). *Management of organizational behavior* (4th ed.). Englewood Cliffs, NJ: Prentice Hall.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Dr. Walter Owen
   Naval Postgraduate School
   Monterey, California

4. John Gay
   Marine Corps Systems Command
   Quantico, Virginia